Caught Between Conscience & Career

EXPOSE ABUSE WITHOUT EXPOSING YOUR IDENTITY

'many lives are at risk'
expensive and wasteful
vulnerable civilians

Acknowledgements

A collaboration of the Project On Government Oversight, Government Accountability Project, and Public Employees for Environmental Responsibility, this survival guide updates the language and lessons from the 2001 book, *The Art of Anonymous Activism: Serving the Public While Surviving Public Service*.

This new edition was made possible thanks to the work of:

EDITOR
Nick Schwellenbach

CONTRIBUTING AUTHORS
Tom Devine
Rebecca Jones
Andrea Peterson
Mandy Smithberger
Timothy Whitehouse

ADVISORS
Kevin Bell
Danielle Brian
Paula Dinerstein
Samantha Feinstein
Dana Gold
Doug Hartnett
Liz Hempowicz
Irvin McCullough
Nicholas Pacifico
Jeff Ruch

COPY-EDITING AND FACT-CHECKING
Danni Downing
Neil Gordon
David Janovsky
Mia Steinle

ASSISTANCE AND RESEARCH
Lane Corrigan
Daniel Van Schooten

DESIGN AND ILLUSTRATION
Rachel Freedman
Leslie Garvey

MARKETING AND OUTREACH
Jordan Bollmann
Abby Evans
Timothy Farnsworth
Andrew Harman
CJ Ostrosky
Pam Rutter

Special thanks to Tom Devine, Jeff Ruch, and the late Beth Daley, who were the main authors of the first edition of this book, and to Frank Serpico, who authored its foreword. And thanks to Andrew Bakaj, David Bralow, Kel McClanahan, Kathleen McClellan, Dan Meyer, Fabio Pietrosanti, Jesselyn Radack, Trevor Timm, Mark Zaid, and Jason Zuckerman for sharing your expertise and experience.

This project was made possible thanks to funding support from Bauman Foundation, CS Fund, Democracy Fund, The Frankel Foundation, Fund for Constitutional Government, Stewart R. Mott Foundation, and Val Schaffner.

Caught Between Conscience & Career

EXPOSE ABUSE WITHOUT EXPOSING YOUR IDENTITY

POGO
PROJECT ON GOVERNMENT OVERSIGHT

GOVERNMENT
ACCOUNTABILITY
PROJECT

PEER

Contents

p. 7 INTRODUCTION

15 BLOWING THE WHISTLE MAY BE HAZARDOUS TO YOUR PROFESSIONAL HEALTH
16 Downsides are Apparent
19 Check Your Parachute Before You Leap: Tips for Whistleblowers
23 Often the Better Way: Delivering the Message, Not the Messenger

25 DELIVER THE MESSAGE, NOT THE MESSENGER
27 Working with Advocacy Partners
36 Liberating Agency Documents with the Freedom of Information Act
38 Harnessing the Collective Voice to Shield Individuals

41 DIGITAL SECURITY FOR WHISTLEBLOWERS
41 Think Before You Click
50 The Current Toolkit

55 **OFFICIAL CHANNEL SWIMMING: STARTING AND MONITORING AGENCY INVESTIGATIONS**
56 Inspectors General
58 Congress
62 Office of Special Counsel
68 The False Claims Act and Other Bounty Programs

71 **THE MEDIUM IS THE MESSAGE**
72 If it Bleeds, it Leads
78 Reporters Are Not Your Friends
79 Yesterday's News

83 **WHISTLEBLOWER LAWS**
86 Federal Civilians
    86 What's a Protected Disclosure?
    90 What's a Personnel Action?
    91 What's Management Knowledge and How is it Proven?
    92 When Can an Agency Claim that the Personnel Action was Legitimate?
    94 Where Can You File Whistleblower Retaliation Claims?
102 Recent Major Federal Whistleblower Laws
103 Protections for Contractors and Other Federal Employees
106 Intelligence Community
112 Military Whistleblower Protections
116 What About the First Amendment?
118 Courtroom Drama: Lawsuits Filed Against Agencies

123 **CONCLUSION**

125 **ENDNOTES**

(5,678,692)
(-418,880)
800,554
50,000
(50,000)
many lives are at risk'
expensive and wasteful
vulnerable civilians

> "The way to right wrongs is to turn the light of truth upon them."

IDA B. WELLS-BARNETT
INVESTIGATIVE JOURNALIST

Introduction

LEGAL DISCLAIMER

The material in this guide is provided for informational purposes only.
Nothing in this publication should be construed as legal advice.
Before you act on any of the material in this guide,
the authors STRONGLY urge you to seek legal counsel.

At government agencies, financial institutions, government contractors, and other powerful organizations, once-lonely voices speaking out against wrongdoing are increasingly being joined by others, and together they are beginning to raise a crescendo that can no longer be ignored or silenced. Institutions that break the law, commit fraud, or harm public health, safety, or security have good reason to fear whistleblowing by conscientious employees. Whistleblowers who "commit the truth"[1] can prompt significant reforms, hold institutions accountable, and shine a light on agency abuses and illegal practices by sparking Congressional hearings, newspaper stories, and prominent television coverage.

Many things have changed since the days of the brown envelope slipped under the door by an anonymous source. Now, the internet and the proliferation of online platforms have expanded the means by which whistleblowers can disclose information and the number of people that information can reach, increasing the potential to make a difference.

Yet many things have stayed the same, particularly the risk that whistleblowers will face retaliation. Further, while the information revolution has expanded whistleblowers’ potential audience, technological advances have also made it harder than ever before to dissent anonymously. In this edition of our book, we’ve considered these new vulnerabilities and other technological developments.

For the purposes of this book, we define “whistleblowers” as individuals who work inside organizations, either in the government or private sector, and who disclose and challenge abuses of power or other failings by their organization that betray the public trust. The whistleblowers can raise concerns purely internally or through disclosures to law enforcement, Congress, other official channels, or the public.

Some people use the term “whistleblower” colloquially to refer to journalists, activists, or others who raise concerns about an organization from the outside. While these individuals often are vital to exposing misconduct, and also sometimes face retaliation from those who are threatened or angered, they are a subset within the universe of “whistleblowers,” and not whom we spotlight in this book.

Moreover, the lessons we present in this book are primarily for whistleblowers working in the federal government, specifically the executive branch. However, the same lessons can be valuable for local and state government whistleblowers, private-sector whistleblowers, and anyone else who wants to bring wrongdoing to light while protecting themselves.

We do not define “whistleblowers” solely as the federal government employees who have legal rights against employer retaliation. Indeed, missing, limited, or ineffective legal protections are major themes in this book. Whistleblower-protection laws have significant loopholes.[2] Further, agencies responsible for turning paper rights into reality do not always have the staffing, resources, or even desire to vigorously enforce the laws, or get it right when they do.[3]

Unfortunately, the public can see whistleblowing through a partisan, ideological, or agenda-driven lens, rather than through one focused on the disclosure’s truth or benefit to society.[4] The latter should be what the public and the government care about. Even if a whistleblower is wrong about the specifics, their disclosures may still warn of valid threats, or an investigation into their concerns may still expose related misconduct.

Deciding to blow the whistle—disclosing information about breaches of public trust through internal channels, publicly, or as an anonymous source—is a professional crossroad after which the employee's career will never be the same. Laudatory press coverage and movie portrayals can sometimes cast whistleblowing in a glamorous light.

Individuals like analyst Daniel Ellsberg, who leaked the Pentagon Papers; FBI agent Coleen Rowley, who blew the whistle on the FBI's failures leading up to 9/11; Enron executive Sherron Watkins, who brought to light the company´s rampant fraud; and scientist Jeffrey Wigand, who exposed dangerous lies by the tobacco industry, are viewed by many as truth-tellers who were successful.[5] But beyond the limelight, these public figures and others who choose to follow their conscience often experience a darker reality.

Retaliation against whistleblowers is widespread and poses a significant barrier to the accountability and transparency of government and corporate conduct. According to government surveys of federal workers in 2010, _approximately one-third of the individuals who felt they had been identified as a source of a report of wrongdoing also perceived either threats or acts of reprisal, or both."[6] An updated 2017 employee survey found that, despite passage of the landmark Whistleblower Protection Enhancement Act of 2012, about 30 percent of government employees say they fear retaliation if they report wrongdoing.[7]

Retaliation against private-sector whistleblowers is also troubling. Despite the enactment of new whistleblower rights following the financial meltdown caused by the home-mortgage crisis of 2007, instances of reprisal against employees for reporting wrongdoing have *doubled* from 22 to 44 percent since 2013, with 72 percent of employees who were retaliated against saying it happened within three weeks of making a disclosure.[8] Research shows that the legitimate fears of reprisal and futility—that speaking up will not change anything—continue to be the dominant reasons employees in all sectors stay silent despite witnessing wrongdoing in organizations.[9]

Federal whistleblower law prohibits managers from taking personnel actions against employees who make any lawful disclosure of information they reasonably believe is evidence of "any violation of any law, rule, or regulation; or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health and safety.”[10] But skepticism and fears of reprisal are justified, because although these protections exist on paper, only a small fraction of employees who filed retaliation claims prevail through the legal process.[11]

Fortunately, legal rights for whistleblowers are steadily getting stronger, and the chances of winning protection have improved. After a thirteen-year campaign by the Make It Safe Coalition, of which our organizations are members,[12] Congress unanimously passed the Whistleblower Protection Enhancement Act of 2012. That legislative makeover of whistleblower rights reversed more than a decade of hostile court rulings, restored access to an appeals process, outlawed agency gag orders, and offered reinforced protection against scientific censorship.[13]

Confusion about whistleblower rights—by employees and managers alike—is widespread.

Similarly, since the 1990s, Congress has passed numerous whistleblower laws providing much of the private sector—including government contractors—with rights enforced through jury trials.[14] Congress’s votes to approve the Whistleblower Protection Enhancement Act and the expansions of corporate whistleblower rights represent an impressive legislative mandate for employee speech rights. This edition of our book keeps pace with new legal developments, and the chapter on the law has been expanded to discuss legal protections for federal contractor, FBI, intelligence community, and military whistleblowers.

Unfortunately, confusion about and lack of awareness of whistleblower rights by employees and managers alike are widespread.[15] And disclosures by employees may anger bosses who face scrutiny as a result.

In sum, whistleblowing continues to be dangerous, and the risk of retaliation remains.

For instance, during the Obama Administration, whistleblower retaliation at the Department of Veterans Affairs made national headlines when the Office of Special Counsel reported a massive surge in whistleblower-retaliation complaints, some from employees who disclosed secret waiting lists that revealed the difficulty many veterans faced in accessing health care at Veterans Affairs medical centers.[16]

In another instance, several agents from the Bureau of Alcohol, Tobacco, Firearms and Explosives asserted that the Bureau retaliated against them for disclosing that a U.S. government operation allowed the sale of thousands of guns that made their way to drug cartels in Mexico.[17] The Bureau settled three of the whistleblowers’ retaliation cases.[18] In the Department of Defense, Army Special Forces Lieutenant Colonel Jason Amerine had his security clearance suspended after he disclosed to Congress how dysfunctional the government’s hostage negotiation and recovery process was.[19] And after Army intelligence analyst Chelsea Manning leaked massive amounts of military and State Department information to WikiLeaks, President Obama commented that Manning “broke the law” before Manning even went to trial before a military judge. Media commentators noted that President Obama may have used “unlawful command influence” because, as the commander-in-chief, he was the judge’s ultimate boss.[20] These are just a handful of examples.

The Trump Administration has also sent chilling signals to whistleblowers. In response to a press question about State Department officials who used the agency’s dissent channel to register concerns with the first version of President Trump’s travel ban, then-White House press secretary Sean Spicer said, “they should either get with the program or they can go.”[21] After an anonymous author who claimed to be a senior Administration official wrote a *New York Times* op-ed critical of the White House, the President called for investigation to find the author.[22]

The retaliation even applies to high-level officials who have left government: President Trump yanked the security clearance of former CIA Director John Brennan specifically for criticizing him, and threatened the clearances of other former intelligence leaders who dissent.[23] As with past White Houses, the Trump Administration has also seen numerous allegations of whistleblower retaliation against rank-and-file employees.[24] Although the numbers peaked with the surge of Veterans Affairs complaints at the end of the Obama Administration, the Office of Special Counsel continues to receive historically high levels of complaints about prohibited personnel practices from federal employees.[25]

Even though both Presidents strengthened legal protections for whistleblowers—and deserve credit for that—these statements and developments during both Administrations may make lower-level employees think twice about speaking up when they witness misconduct, and certainly about identifying themselves.

Most frightening, government employees who disclose information to the press are encountering criminal investigations and prosecutions, illustrated by record levels of prosecutions of government employees under the Espionage Act. President Obama's Justice Department used the law to prosecute more government officials who had made disclosures to the press than all past Administrations combined.[26] Under President Trump, the Justice Department ramped up leak investigations, tripling the number during the first year of the Administration, according to then-Attorney General Jeff Sessions.[27] A top Justice Department official stated in June 2018, "The Attorney General has stated that investigations and prosecutions of unauthorized disclosure of controlled information are a priority of the Department of Justice."[28] As of February 2019, four of the six prosecutions of employees for disclosing classified or otherwise sensitive information to the press during the Trump Administration involved "disclosures related to Trump, the circle of people around him, and the Trump-Russia inquiry," according to *The Intercept*.[29]

Another alarming fact is that due process and legal remedies available for many types of whistleblowers are woefully inadequate. For instance, unlike corporate and government contract workers, federal employees cannot seek justice against whistleblower retaliation through jury trials in courts.[30]

Perhaps the starkest choice government employees may confront is if they should overlook violations of law or obey a direct order to violate the law. The government employee is faced with an unpalatable choice of possible discipline for insubordination or potential liability for knowingly sanctioning violations of law. While federal civil service protections make it illegal to retaliate for refusing to violate a law, rule, or regulation,[31] the lack of credible due process means in practice that law-abiding public servants still proceed at their own risk.

This bleak reality means that those seeking to expose and resolve problems caused by corruption, political pressure, unaccountable bureaucracies, incompetence, or illegal actions within government agencies and by powerful corporations should do so in ways that are less risky for their careers, if possible.

Caught Between Conscience and Career is intended to help employees encountering these difficult ethical issues in their workplaces and to empower them to make the best choices. It is a survival guide for whistleblowers. It walks through the difficulties that may be encountered when blowing the whistle, the path of disclosing information without disclosing your identity, how to securely communicate electronically, the pros and cons of different official government channels for disclosure, tips for working with the press, and a primer on legal protections.

The most important point is that it is possible to fight wrongdoing from within without sacrificing your career.

There is a desperate need for conscientious employees to serve as the public's eyes and ears about what is happening within powerful organizations. The vitality of the United States' democracy, the long-term viability of its economy, and public health, safety, and security depend upon truth-tellers to shine light on corruption and malfeasance.

There is a vibrant community of concerned citizen-activists who seek to aid those patriots who struggle to serve the public good.

Three organizations with many decades of experience supporting whistleblowers have contributed to this guide—the Government Accountability Project, Project On Government Oversight (POGO), and Public Employees for Environmental Responsibility (PEER). We can help you bring serious problems in the federal government and the private sector to light by providing assistance in exposing wrongdoing; assistance in conducting policy advocacy and media campaigns to remedy identified problems; and investigative research. The Government Accountability Project and PEER provide legal assistance and representation to whistleblowers as well. Collectively, we have helped countless conscientious employees do the right thing while still minimizing the risk to their careers.

If you blow the whistle, first learning the lessons of others who suffered can make all the difference in your own efforts. We hope this guide — reissued with new and revamped information for the 30th anniversary of the Whistleblower Protection Act — will be an effective course in how to "commit the truth," a phrase coined by the late, legendary Pentagon whistleblower Ernie Fitzgerald.[32]

TOM DEVINE
Legal Director, Government Accountability Project

DANIELLE BRIAN
Executive Director, Project On Government Oversight

TIMOTHY WHITEHOUSE
Executive Director, Public Employees for Environmental Responsibility

SUBJECT: Reprimand
CHARGE: Inappropriate Conduct
1. You are reprimanded for the following reason:

> "If you're going to sin, sin against God, not the bureaucracy. God will forgive you but the bureaucracy won't."

ATTRIBUTED TO

ADMIRAL HYMAN G. RICKOVER

1

Blowing the Whistle May be Hazardous to Your Professional Health

In the spring of 2014, whistleblowers at the Department of Veterans Affairs (VA) came forward and told the press horrific stories of how veterans were not receiving the medical care they needed. This sparked a deluge of disclosures by others across the VA that led to front-page stories, cable news investigative exposés, and Congressional hearings. Veterans Affairs Secretary Eric Shinseki and others resigned in the immediate wake of the scandal.[1]

But many of the whistleblowers who raised concerns also faced retaliation from the federal government. The Government Accountability Office issued a report in the summer of 2018 that found VA whistleblowers were "10 times more likely [than VA employees who don't blow the whistle]...to receive disciplinary action within a year of reporting misconduct."[2]

Too often, the more successful whistleblowers are at making a difference, the more threatening they become to those whose actions cannot withstand scrutiny. Their successes can motivate retaliation if they are identified. And for those who think that blowing the whistle publicly is glamorous or a path to recognition, think again. Many whistleblowers suffer in obscurity, frustrated by burned career bridges, blackballed in their line of work, and never achieving the validation they sought. For every success story, there are an untold number of stories of professional martyrdom. The prominent, lionized exceptions stand as beacons of false hope for thousands.

Few paths are more professionally treacherous than challenging abuses by your own employer.

Whistleblowing is always dangerous, but embarking on that path without preparation and thoughtful consideration of the consequences can be a recipe for disaster.

For those contemplating (or maybe unable to avoid) being identified as a whistleblower, we sketch out some considerations and potential negative consequences in the following pages. Sometimes whistleblowers avoid worst-case scenarios, but you shouldn't expect to do the same: it is better to be prepared and be pleasantly surprised.

Downsides Are Apparent

It takes individuals to deliver the truth about wrongdoing and sometimes the only individuals in a position to do so work within the very organizations committing wrongdoing. But few paths are more professionally treacherous than challenging abuses by your own employer. If you are thinking of publicly opposing an action by your agency or openly reporting wrongdoing in the workplace, here are some considerations to think about before acting.

IT IS NOT A FAIR FIGHT

One person against a government agency is inherently a David-versus-Goliath struggle. The organization holds most of the cards. People who speak out loudly and publicly against their organization can face repercussions in their jobs. Not all of these repercussions are immediately obvious. Some whistleblowers are given lateral transfers to isolated or unpopular offices.[3] Some organizations relentlessly create a hostile workplace where they are socially ostracized.[4] Some are scrutinized by management that seems to be looking for problems.[5] Still other whistleblowers find that they are passed over for promotions.[6]

The tactics for harassing whistleblowers are manifold. For example, an organization can:

- **Set an employee up for failure.** Usually, this means giving the employee impossible assignments and then firing or demoting them for non-performance.[7]

- **Blacklist the employee so that they cannot find gainful employment in their chosen field.** That employee then serves as an example to scare off others from the same fate.[8]

- **Conduct a retaliatory investigation[9] and charge the employee with an offense as minor as stealing pens.[10]** Smears of alleged misconduct similar to what the whistleblower is challenging are common, potentially to undermine the whistleblower's credibility and make them look like a hypocrite. Significantly, federal whistleblower law does not allow employees to challenge retaliatory investigations until there is a subsequent personnel action.[11] Whistleblower protections only create protections from adverse employment-related actions, such as terminations and demotions, and do not shield against criminal prosecutions. That means they have no anti-retaliation rights against this not-uncommon tactic. The criminal charges whistleblowers have faced have ranged from theft or misappropriation of government property to violations of the Espionage Act.[12]

- **Discredit or humiliate the whistleblower by questioning their mental health, professional competence, reliability, or honesty.** One tactic is to order the employee to undergo a psychiatric examination. Often the agency can hide behind privacy laws to hint that there is a problem with the employee that the agency is not at liberty to disclose.[13]

IT OFTEN MISSES THE POINT

When agency employees go public with tales of malfeasance or other information of public concern, the media spotlight may focus on the personality at the expense of the issue. Whistleblowers may find that they become the story.

There are a number of problems with this.

Government agencies often find it easier to distract from their misconduct by attacking the messenger than addressing the message. Rather than face the problems brought to light, managers may simply try to focus attention on the "disgruntled" employee."[14] The conscientious worker is then portrayed as vengeful, dishonest, and self-serving. Women can face misogynistic accusations and racial minorities can face racist allegations.[15]

This allows the agency to turn the tables and put the employee, or their motives, on trial: Is the whistleblower a good employee? Does the whistleblower have a hidden agenda like revenge or ambition? In many instances, the whistleblower's work record is irrelevant to the issue at hand, but it can occupy center stage in terms of public attention.

In instances where the employee is fighting to obtain a remedy for retaliation, the case turns on questions of employment law (see Chapter 6) such as: Was the termination lawful? Is there a legitimate reason for the transfer? Did the agency abuse its discretion? The concern the employee raised becomes a subsidiary issue in a reprisal case. This means whistleblowers must fight on two fronts ˆ to defend themselves, and to convince government authorities to address the problems they raised.

IT OFTEN TAKES THE BEST AND BRIGHTEST OUT OF THE ORGANIZATION

Good professionals are often casualties of whistleblower conflicts. Even vindicated whistleblowers leave agencies as a matter of survival, or are too disheartened to continue in their chosen career.[16] Usually, it is not realistic for an employee to work for a boss they just battled. In those instances when a whistleblower can obtain a transfer for a fresh start in the organization or industry, the whistleblower's reputation will likely follow. At a minimum, agency managers will likely shy away from giving whistleblowers sensitive or potentially controversial assignments—in other words, the most significant work where integrity counts the most.

If a whistleblower files a legal complaint and if it results in a positive outcome, agencies often pay them to leave as the case´s final resolution. But conscientious employees who take career risks to address problems are precisely the people who best serve the public, and are the employees we need to keep in government agencies.

The human dimension to these risks should not be overlooked. Being a whistleblower is stressful.[17] Whistleblowers have reported impacts on personal relationships, ranging from friendships to marriages.[18] Less obvious but no less real is the strain from "mind-game" retaliation. As employees are transferred to less-interesting projects or have their responsibilities removed, boredom and frustration can set in. Supervisors may overly nitpick at an employee's work product. Once-friendly colleagues may suddenly ostracize a whistleblower as word gets around that they are on management's bad side.

CHECK YOUR PARACHUTES BEFORE YOU LEAP

Tips for Whistleblowers

Notwithstanding the above, you may choose to blow the whistle. As we explain in later chapters, often employees do not even think they are engaging in dissent, believing they are just doing their jobs. But then they wake up one day to find that they somehow made the transition from valued worker to Public Enemy Number One. In other instances, the employee is in a situation where they have nothing to lose by fighting.

When that moment of realization or decision arrives, pause for a moment to review the following survival tips that apply to whistleblowers who choose not to act anonymously.

CONSULT YOUR LOVED ONES

Blowing the whistle can impact your entire family. Before taking any irreversible steps, talk to your spouse, significant other, family, or close friends—the support group you will need in the coming days, months, or years—about your decision to blow the whistle. If they are not with you, you may want to rethink this path.[19]

CHECK FOR SKELETONS IN YOUR CLOSET

Any personal vulnerability or peccadillo can be used against you by your agency. If there is something in your past you do not want to see on the front page of the newspaper or shared with the world on social media, reconsider blowing the whistle. One practical step is to make a copy of the complete contents of your personnel file as insurance that your employer cannot later slip new but backdated “dirt” into it.

DOCUMENT, DOCUMENT, DOCUMENT, BUT BE CAREFUL

Keep copious records and a daily diary of relevant information to memorialize conversations and developments. Forward or print relevant work emails and maintain copies of records in case you are cut off from evidence in your workplace that can assist you in proving your allegations. Your chances of success will likely depend on how powerful a paper trail you produce.

Be warned, however. Proving your charges with institutional records can be extremely dangerous. It can mean criminal prosecutions for unlawfully copying or removing government records. There have even been cases where federal employees have been threatened with prosecution for sharing non-classified information.[20] See Chapter 2 to learn more about the risks of disclosing classified information. Corporations aggressively file multi-million dollar "SLAPP suits"[21] or seek criminal prosecution against employees for allegedly stealing company property, even if it is evidence of the organization’s criminal misconduct.

Depending on the potential legal liabilities involved, whistleblowers should store their copies of evidence in a secure, independent location away from their homes, preferably through an attorney where confidentiality is generally protected by attorney-client privilege.

If there is any doubt, a safer tactic may be hiding copies of paper records on the organization’s premises in a location that will not draw attention, such as archives or some other innocuous location. Copies of electronic records can be stored under misleading folder names or in locations that are unlikely to be discovered (see Chapters 2 and 3 for more discussion of the risks of moving agency records). That way the whistleblower can be a navigator for law enforcement authorities, instructing them on what records to seek, and then where to find them if an employer denies their existence.[22]

DON’T USE YOUR EMPLOYER’S RESOURCES

Avoid using your employer´s resources for making a disclosure or filing a retaliation claim.

Your work phone, computer, copier, and any other institutional resources all belong to the agency, and it is likely that if you use those resources to make a disclosure or file a retaliation claim, identifying information will be in management's hands soon after you blow the whistle.[23]

Time is also an institutional resource. Depending on the circumstances, you could end up enabling your organization to make the argument that you committed time fraud, misappropriated agency time or resources, or simply are a poor performer.[24] Unless you have specific approval, such as through a union collective bargaining agreement, you also may not be able to use work time to prepare a defense for yourself in a retaliation case.

Even off the clock, you also should make it clear that you do not speak for the agency—especially if you are communicating concerns to the press.

CHECK TO SEE WHO, IF ANYONE, WILL SUPPORT YOUR ACCOUNT

Solidarity is important for your ability to make a difference and survive professionally. Do not wait to be cut off by your agency.

Without exposing yourself as a threat to the organization, gauge the level of support among your co-workers for the concerns you might raise. See if others share your concerns.

This is important for quality control, not just for your sense of solidarity. They may have knowledge to which you were not privy, and that could change your mind or modify or expand your concerns. Get a sense of whether key people will back up your account. If you can't count on others to later testify as supporting witnesses, you may be well advised to wait before challenging misconduct. Try to stay on good terms with administrative staff who may be in a position to know of impending agency actions.

Seek out potential allies before your situation heats up, and work through intermediaries when possible. Enlist the assistance of sympathetic interest groups, elected officials, or journalists. The strength of your support coalition is often key to making the legal rights you have on paper work for you in reality.

CONSULT AN ATTORNEY EARLY

Do not wait until you are in the "career emergency room" before seeking professional help. As with preventative medicine, getting a little legal advice up front can protect against the need for extensive intervention later. Be careful to find an attorney who respects your goals as a whistleblower, and who is willing to safeguard your evidence. Many attorneys see their duty as preventing you from incurring the liability you are willing to risk but that you should be prepared for. This will be an intimate professional partnership, so make sure you trust and are compatible with your lawyer. One reason some whistleblowers hire attorneys is because they can make disclosures on behalf of an anonymous client, legally shielded by attorney-client privilege.[25]

CHOOSE YOUR BATTLEGROUND CAREFULLY

If possible, pick a time and set of circumstances where you will have the most impact with your disclosure. The timing of your disclosure, particularly to the press, is a serious strategic decision that can affect the chances your disclosure will receive attention. Timing can also affect whether you face retaliation. Press coverage can cut both ways: it could shield you from immediate retaliation while you remain in the media spotlight, but it could also anger your management more than if your disclosures were more discreet.

If you do decide to disclose your evidence to the press, it may be wise to release your evidence incrementally rather than all at once. This can spark repeated stories that sustain the spotlight, and provide a chance to call the bluffs of overly broad institutional denials. See Chapter 5 for an extended discussion of working with the press.

HAVE A WELL-THOUGHT-OUT PLAN

Those who are abusing their power must be reacting to you, not vice versa. Otherwise, you will get overwhelmed by the agency’s superior resources, access to information, and political clout, and its presumed institutional credibility.

Be clear-headed about precisely what you expect to accomplish and how. Do not premise your actions on the vague notion that the truth will prevail. Plan out a step-by-step scenario of what documents should be released when, and how your organization’s responses will be perceived by key audiences such as the press or government oversight bodies. As part of your advance work, get information into the hands of key potential organizational and political allies, and earn their commitment to reinforce your disclosure. Try to prepare for your management's counter-moves by anticipating agency reactions to your charges and by mapping out the response to those moves. The tenor of this first exchange may determine if the immediate battle with your organization will be quick or drawn-out.

DEVELOP AN EXIT STRATEGY

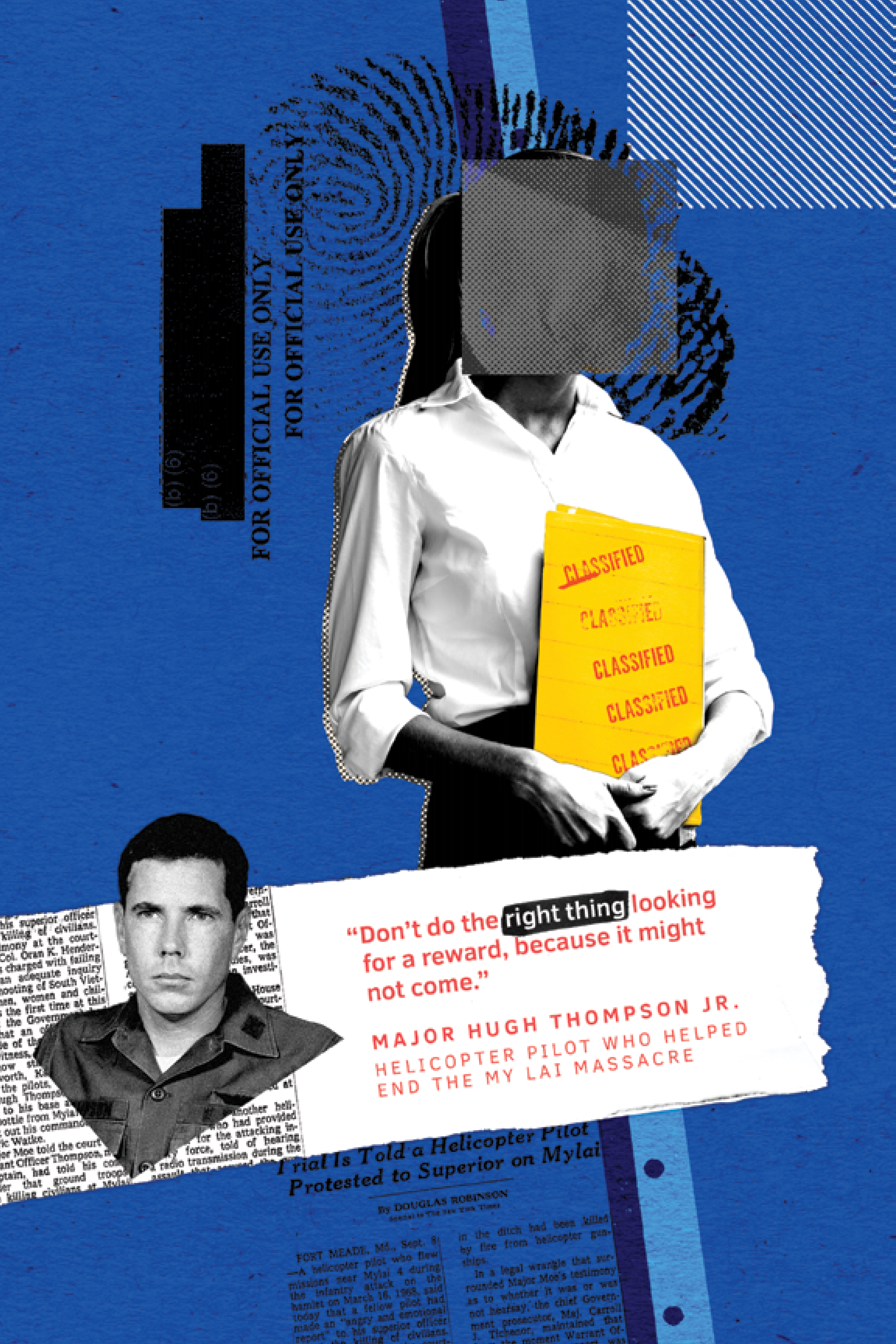
Map out where your actions will leave you a year from now, two years from now, five years, and further on. Plan out the route you want to take and how you reasonably expect your professional path to proceed. There is little doubt that you are about to embark upon a journey that will have a significant impact on your professional and personal life, and you should be prepared with a realistic roadmap of how you might get where you want to go in your career. However, you should also have contingency plans since once you make a disclosure, particularly if it becomes public, your career and life may change in unexpected ways.

OFTEN THE BETTER WAY

Delivering the Message, Not the Messenger

Throwing away your entire career, particularly if there are other ways to air the problem, can be imprudent and counterproductive. In addition, bureaucracies prefer to focus on the “disgruntled employee” rather than the substance of the problem. The longer you can keep the spotlight on the issue and not on you, the greater the chance the problem will be addressed, the longer you will maintain access to evidence necessary to prove your concerns, and the greater the chance you can keep your job and avoid retaliation.

As discussed in the next chapter, you can bring agency troubles to light by focusing on the message without making yourself the target of management's anger. The best way to do this is by providing powerful evidence to those who can expose the wrongdoing and take action without leaving an obvious trail for managers to trace back to you.


FOR OFFICIAL USE ONLY
FOR OFFICIAL USE ONLY
(b) (6)
(b) (6)
CLASSIFIED
CLASSIFIED
CLASSIFIED
CLASSIFIED
CLASSIFIED

> "Don't do the **right thing** looking for a reward, because it might not come."

MAJOR HUGH THOMPSON JR.

HELICOPTER PILOT WHO HELPED END THE MY LAI MASSACRE

Trial Is Told a Helicopter Pilot Protested to Superior on Mylai

By DOUGLAS ROBINSON
Special to The New York Times

FORT MEADE, Md., Sept. 9—A helicopter pilot who flew missions near Mylai 4 during the infantry attack on the hamlet on March 16, 1968, said today that a fellow pilot had made an "angry and emotional report" to his superior officer

in the ditch had been killed by fire from helicopter gunships.

In a legal wrangle that surrounded Major Moe's testimony as to whether it was or was not hearsay, the chief Government prosecutor, Maj. Carroll J. Tichenor, maintained that

2

Deliver the Message, Not the Messenger

One way you can spur change at your agency is by releasing information about wrongdoing while staying under the radar.

In order to be anonymous, you must shield all of the identifying information that can be traced back to you, not just your name, from public disclosure and from your management. Your desire to remain anonymous may force you to make some high-stakes choices on what information to disclose.

In some instances, the evidence that reveals agency misconduct also inherently reveals the whistleblower source, such as a sensitive memo with an extremely limited circulation or an email sent to only a few recipients. In other words, when few people know the truth, the facts can be the equivalent of your signature. In these cases, you could suffer career damage if your agency learns that you were the employee who released the information.

Unless the information you're disclosing has titanic significance, risking your career in order to expose one act of misconduct is hard to justify.

The key then is to stay undercover and work on your own time with others, such as an advocacy group or journalist, to share the critical information in a way that leaves no fingerprints (or as few as reasonably possible). Strict confidentiality procedures coupled with ready legal assistance can help maximize your protection.

In short, anonymity prevents retaliation. Anonymity does not necessarily mean that reporters, advocacy partners, or Congressional staffers you choose to work with will not know your identity. In this book, we generally use "anonymous" to refer to whether your agency or the public knows you are a whistleblower.

Anonymity does not necessarily mean that reporters, advocacy partners, or Congressional staffers you choose to work with will not know your identity.

Being anonymous also allows you to keep your job and to access a sustained flow of information from your agency. If you are able to maintain your anonymity, you may get advance access to any organizational strategy to deny or cover up your anonymous disclosures. This insider role is especially powerful if you are the organization's expert on the topic and your knowledge is needed to craft the response.

Needless to say, being on the organization's damage control team can be especially advantageous in keeping a controversy alive—you can expose deliberate misstatements your agency makes to the press or to Congress. This can keep authorities or the public a step ahead of government attempts to perpetrate a cover-up. By contrast, once you're exposed as a threat, the flow of information to you will dry up.

Techniques that have been effective at shielding identities and getting the truth out for past whistleblowers include working with advocacy partners, using the Freedom of Information Act to get documents released, and working through collective action to shield individual whistleblowers.

Whether you're working with journalists, advocacy groups, or Congressional staff, you should pin down specific confidentiality commitments before exposing yourself to risks. Some groups less sensitive to the plight of whistleblowers may choose to risk exposing your identity for what they believe is the greater good. Congressional staff may not realize they are exposing you when they demand answers from agencies by asking questions that sound like the points you are known to have made internally. Because of the great risks that come with whistleblowing, it is important to make a plan with a trustworthy advocacy group or publishing partner to prevent your exposure.

Sometimes developing and implementing such a plan takes weeks, months, or even years. Considering the alternatives, however, the wait and effort in planning are well worth it.

Working with Advocacy Partners

Having external allies and public opinion on your side can help you safely and effectively bring the truth to light. Advocacy partners can be a networking lifeline to neutralize workplace isolation, whether you are a secret source for disclosures and thus cannot talk to anyone at work about what you are doing, or you become ostracized because management identified you as the source. An outside group can help provide you with resources, connections, and assistance in developing a constituency for the truth about abuses of power your agency is hiding. This outside affiliation can be key to effectively utilizing your limited time outside of work.

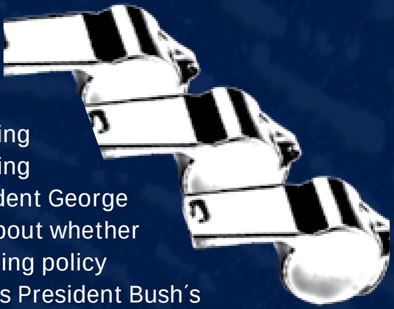
An advocacy partner may be a union, nonprofit organization, or professional society.[1] Whatever you choose, it is essential that you trust that the partner shares your goals and priorities, including minimizing negative consequences to you, so that your concerns and welfare are not subordinate to a pre-set agenda. An advocacy partner can work with you, your attorney, reporters, or any other players relevant to getting the truth out, such as Congressional committees.

It is essential that you trust that the partner shares your goals and priorities, including minimizing negative consequences to you.

The advocacy partner can act as both a shield to protect your identity and a conduit for your information to get to the outside world so that your concerns become known and hopefully acted-upon. This partner may also be able to identify allies within your organization.

Take the classic example of a leaked document. A document detailing disconcerting information the public should know about has been broadly circulated within an organization.[2] An employee who wants to make sure this document enters the public domain could try to contact a reporter directly, or could entrust it to an advocacy partner.[3] The partner could negotiate terms for its use with the reporter, organize others to comment about it on the record, and publicly follow up by pushing the agency to respond.[4]

LEAVING NO FINGERPRINTS



As an oil-industry favorite with a history of pro-drilling advocacy, Gale Norton faced skeptical Senators during her confirmation hearings in 2000 to serve as President George W. Bush´s first Interior secretary.[5] She was grilled about whether she could set aside her personal views when evaluating policy decisions, particularly on high-profile issues, such as President Bush´s proposal to drill for oil in the Arctic National Wildlife Refuge. To allay those concerns, Norton unequivocally pledged to relay “the best scientific evaluation of the environmental consequences” from oil development in the Refuge.[6] She lied.

After her confirmation, Alaska Senator Frank Murkowski wrote to Norton requesting her department´s assessment of the effects of oil drilling on the Porcupine caribou herd in the Refuge. Norton directed Murkowski’s questions to the Fish and Wildlife Service, an agency within the Interior Department that oversees the Refuge. The Fish and Wildlife Service reported its conclusions back to Norton but the conclusions did not suit her—so she doctored the responses.[7]

Fish and Wildlife Service employees contacted Public Employees for Environmental Responsibility and provided the group with the paper trail consisting of two letters: one from the Service to Norton, and the other from Norton back to Murkowski. The contrast between the letters is stark. Norton made substantive changes to the scientific findings. All of Norton´s changes were designed to minimize the impacts of the projected drilling activity.[8]

An exposé in *The Washington Post* ran on the very day Norton was giving a keynote speech at the Society for Environmental Journalists conference in Portland, Oregon.[9]

Norton admitted that “we did make a mistake,” but ascribed discrepancies to an error made when copying information.[10] A spokesman for Norton also admitted they had set aside the Fish and Wildlife Service´s scientific findings, claiming she was relying on other“peer-reviewed” data.[11] In fact, the data she used was from a non-peer-reviewed study by an academic who often worked for oil companies and who acknowledged oil giant BP Exploration for providing “encouragement, funding and useful comments” on his research.[12]

This episode helped sink the effort to open the Refuge for drilling during the George W. Bush Administration.[13] Moreover, the sources of the original documents were never revealed.

The episode gained new relevance during the Trump Administration with the nomination of a former Norton political aide, David Bernhardt, to be deputy Interior. Bernhardt´s legislative affairs office had sent Norton´s misleading letter to Congress.[14] When Hawaii Senator Mazie Hirono asked in a May 2017 hearing about Bernhardt’s contribution to Norton’s misleading letter, he responded with little more than that his office had engagement at each stage and ultimately transmitted Norton’s letter to Congress.[15] He subsequently was confirmed as deputy secretary. As of this book’s publication, he was on a verge of a promotion. In early 2019, President Trump nominated him to be Interior secretary.

It could use the whistleblower's evidence as the basis for a public campaign that amplifies the whistleblower´s revelations by posting documents online, issuing press releases and investigative reports, or placing relevant opinion pieces in news outlets.

In other words, it helps to have friends. But remember, each advocacy organization has its own agenda. Even if your interests appear to be aligned, the organization has no formal obligation to be loyal to you. Thus, you may want to establish a formal attorney-client relationship with an attorney at an advocacy organization.[16] An attorney-client relationship means that the attorney must work with your best interests in mind. The relationship is covered by the attorney-client privilege,[17] which generally requires the attorney not to disclose certain information you share with them.[18]

The privilege generally shields information from being released, but can be challenged in court if there is some factual basis showing that an attorney gave advice related to committing a future crime.[19] Given that the federal government has prosecuted employees for disclosing classified and other restricted information, it is important for the whistleblower to discuss the extent of his or her personal liability and the potential liability of the attorney regarding the dissemination of leaked information.

You should be careful not to disclose any restricted information to the attorney until the attorney advises you regarding liability; as noted below, there are many scenarios in which a disclosure is protected only if it is made to certain recipients, which often does not include private attorneys.

Make sure you are comfortable with how little control you may have once you hand over information.

Not all advocacy organizations will legally represent whistleblowers, though. Further, there can be conflicts between the group's interests and the whistleblower's. When that happens, one party or the other must waive its rights, and the advocacy organization may not want to hamper its options. So, another course is to seek out your own attorney who can act as an intermediary between you and an advocacy organization. The attorney can shield your identity, serve as a go-between for communications, and make sure your interests are not sacrificed.

If you share information with an advocacy group or others anonymously and without legal representation, those communications are inherently less controlled. Unless you obtain an advance agreement on conditions for the

KEEPING THE GENERALS FROM GETTING TOO COMFORTABLE

After the 9/11 terrorist attacks, U.S. counterterrorism spending surged, ostensibly to keep Americans safe.[20] Not all of that money was used that way. An example of how counterterrorism funds were being diverted came to light in 2008.

A source inside the federal government provided the Project On Government Oversight with documents showing that the Air Force was building “world class” accommodations on military aircraft for senior military leaders. These accommodations were called “Senior Leader In-Transit Comfort Capsules,” and were designed to be “aesthetically pleasing and furnished to reflect the rank of the senior leaders using the capsule,” according to the documents.[21] These comfort capsules featured leather chairs, flat screen monitors “of at least 37 inches,” and automatically adjusting ambient lighting. One Air Force general ordered the wood to be replaced with cherry, and the brown leather to be ripped out and replaced with Air-Force blue. The millions of dollars needed for the project came out of counterterrorism funding.[22]

POGO worked with *The Washington Post* to break the story.[23] A flurry of other media coverage followed, including a *New York Times* editorial and a segment on The Colbert Report.[24] Senators John Warner, John McCain, and Claire McCaskill all questioned the program.[25] The Air Force scaled back its plans.[26]

material you provide, the organization has a blank check to use the information however it wants, without regard to or even knowledge of the consequences for you the whistleblower. So make sure you are comfortable with your partners and how little control you may have once you hand over information.

You may not need counsel, but at a minimum you should have an explicit conversation with the advocacy partner about your concerns, and you should feel that you’re dealing with honest brokers whom you can trust with your professional life. In this situation, it may be difficult to stay anonymous to the advocacy organization’s staff, who may want to know who they’re talking to (this does not mean they will reveal your identity externally; the same goes for reporters, Congress, and official oversight offices). Even if you feel you can negotiate on your own with the advocacy organization, it may add a layer of comfort to have an attorney who's working for you be part of the process. They may point out considerations you have not thought of.

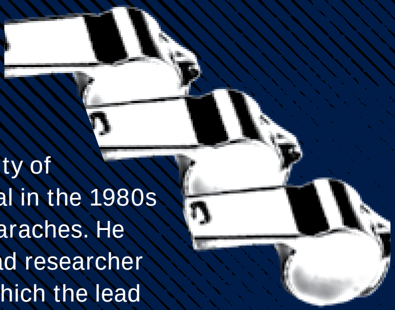
There are some additional cautionary notes to consider before you hand over documents to an advocacy group. See Chapter 3 for details on how to minimize your digital fingerprints when moving evidence from your agency to an advocacy partner or anyone else.

Some whistleblowers, ideally using secure methods, email pertinent documents from their agency to their personal email account or a private digital drop box, ostensibly to be able to work at home but simultaneously to preserve copies of "smoking gun" documents in case the agency later deletes the originals. Before doing so, check to make sure there are not restrictions on emailing or otherwise moving the government documents you need.[27] Also, it can be very dangerous to possess the documents at home, where you are vulnerable to the authorities ransacking your house. You need to be especially careful with how you handle classified information (see the section below on the risks of classified information) or information that the law specifically prohibits public release of,[28] such as material covered by the Privacy Act or medical-patient privacy protections.[29] Remember, as noted earlier, your agency can see how you use government resources such as government computers, networks, printers, copy machines, or email accounts, so emailing yourself files or printing them at work means your agency may be able to identify you.

If you are not careful, your agency could target you for improperly taking possession of restricted information.

If you are not careful, your agency could target you for improperly taking possession of restricted information.[30] From the standpoint of your legal liability, a safer way to prevent destruction of documents is to secure them within the workplace, mixing them in with archives about different topics or electronically filing them under a misleading, innocuous title. Even this is not foolproof. Your agency may have rules on how government information must be secured even if the information does not leave the workplace, so you should consider that as well.

If you decide that removing evidence is necessary, you may want to consider hiring your own lawyer and asking them if they can maintain the files,



AMPLIFYING INSIDER VOICES

Dr. Erdem Cantekin was a researcher at the University of Pittsburgh working on a federally funded clinical trial in the 1980s evaluating the efficacy of antibiotics on children's earaches. He became alarmed when he realized that the trial's lead researcher was misrepresenting the results of the research—which the lead researcher began doing after he personally received honoraria and $262,000 in funding for travel expenses from drug companies making the antibiotics. While Cantekin's data showed no advantage to the use of antibiotics over that of a placebo, the lead researcher presented the data to support of the use of these antibiotics.[31]

When Cantekin raised his concerns, his university tried to suppress him. This eventually sparked a Congressional investigation and examinations by the National Institutes of Health (NIH), which had provided over $17 million to fund the research. One NIH review found the lead researcher had "analyzed the data from NIH-funded research in a manner biased toward the effectiveness of the antibiotics he had evaluated with public monies."[32]

Cantekin's disclosures also triggered a decades-long series of retaliatory measures by the University of Pittsburgh, including the removal of his research responsibilities and a salary freeze at its 1986 level.[33]

In the 1990s, Cantekin began working with the Project On Government Oversight (POGO) to help expose the misinformation spread by drug companies who reap billions of dollars in antibiotic sales. Together, Cantekin and POGO released a report in 1994 that convinced an agency within the Department of Health and Human Services to change its guidelines: the new recommendation was for pediatricians to include "watchful waiting" as an alternative to prescribing antibiotics for children's earaches.[34]

and if attorney-client privilege would shield the files. Please note there's a caveat: attorneys cannot legally receive all restricted information that potentially is provided to them, such as classified documents.[35] You can also seek an attorney's advice on the safest way to get your information to an advocacy group or others. Another way to get documents in the hands of an advocacy partner is to help the partner craft a Freedom of Information Act request to your agency (see "Liberating Agency Documents with the

Freedom of Information Act" on page 36 for more).

Smoking guns and proof of cover-ups make a difference. By working with an advocacy partner, you can inform the public of the existence of incriminating documents or other evidence of malfeasance. Public awareness is often the key to holding government entities accountable for malfeasance.

Handing over evidence is only one of the ways you can work with advocacy partners. Another is educating them on the complicated bureaucratic issues, abuses of power, or violations of law that you have witnessed. While these problems can seem arcane to the general public, they often have profound impacts on public policy, and an advocacy group may be able to translate your specialized knowledge in a way that the public can easily understand.

Another option for educating the public is to submit a public comment in a federal rule-making process, as long as you do so outside of work time and using non-governmental equipment. But some offices are so politicized that many employees dare not participate in that process. And unless your comment has information protected by whistleblower laws, federal employee speech outside of the workplace on issues related to their job falls into a gray zone of First Amendment protections—meaning that you can't rely on the Constitution to protect you from on-the-job repercussions (see Chapter 6 for a detailed discussion of legal protections).[36]

Another way you can get insider expertise out into the public domain is to publish white papers anonymously, with the help of an advocacy partner's edits to ensure the issue makes sense to the public and the media. A white paper provides a lay translation of technical terms and concepts, and provides context for the details of an organization's malfeasance or other actions that have a detrimental impact on the public. The result is a media- and public-friendly report that could only have come from an insider. These employee-written white papers have formed the basis of litigation, been the subject of legislative hearings, and helped shift the tide of policy.

Similarly, you can anonymously draft public comments, administrative appeals, document requests, or letters for signature by the advocacy group. You remain anonymous, of course. But the advocacy partner works with you to ensure that the facts are well documented. This includes citing publicly available materials and referring to—or even appending—reproduced copies of internal memos not easily available to the public (see Chapter 3 on how to minimize risks when using electronic communications and digital devices).

THE RISKS OF CLASSIFIED INFORMATION

If you transmit classified information to an advocacy group or anyone else not lawfully authorized to receive it, you risk felony prosecution under numerous laws,[37] including the Espionage Act.[38] Although you may send the information anonymously, there often is encrypted, invisible tracing information that can lead right back to you. The organization that receives the information may face legal risks as well, depending on the circumstances. Unless you are willing to eventually pay the price in potential criminal penalties, you should not try to send classified information to an advocacy partner or others not authorized to receive the information. At the very least, you should have a serious discussion with your intended recipient before revealing classified information to them.

In the Government Accountability Project's experience working with national security whistleblowers, the Project has never come across misconduct that cannot be credibly, effectively summarized in an unclassified manner. It may take classified information to prove a charge, but not to allege there is an abuse of power or other misconduct. As we discuss in this book, you may then be able to bury the incriminating documents in agency files where law enforcement authorities can find them if the institution denies their existence. The Government Accountability Project strongly advises whistleblowers against sending or providing it classified information because of the legal consequences.

An example of safely raising concerns about a classified program in an unclassified way involves John Tye, a former State Department official, who worked with attorney Mark Zaid to safely reveal the privacy and constitutional concerns created by surveillance authorized by Executive Order 12333 in a piece published by *The Washington Post* in 2014.[39] Tye had more leeway to speak publicly because he was a former official, but he also protected himself from potential prosecution. He and Zaid submitted a draft of the piece to "a pre-publication review by the State Department and the [National Security Agency] to ensure the op-ed did not contain classified information," according to *Vice*, a media outlet.[40] "They didn't redact a damn thing," Zaid told *Vice*. Soon after Tye's public disclosures, the Executive Branch's Privacy and Civil Liberties Oversight Board launched a review of the surveillance programs authorized by this executive order.[41]

A less-successful example can be seen in the case of John Reidy, a former CIA official, who worked with attorney Kel McClanahan in an attempt to safely reveal the existence of a "'catastrophic failure' in the spy agency's operations."[42] In that case, the CIA pushed back against every attempt Reidy and McClanahan made to follow the rules, at one point even refusing to grant McClanahan access to the relevant classified information in Reidy´s appeal to the Inspector General of the Intelligence Community.[43] This meant that McClanahan was excluded from any interviews with government officials about Reidy´s whistleblowing efforts. Even after investigative reporters in 2018 revealed details of the intelligence failure Reidy had blown the whistle about,[44] he remained unable to confirm any information either to the media or to his own lawyer.[45] Despite the disadvantages these restrictions imposed, Reidy remained insulated from more punitive measures, such as criminal prosecution.

Good-faith efforts to avoid using

classified information can also lead to nightmare situations. Take the example of then-National Security Agency official Thomas Drake, who disclosed what he believed was unclassified information about a wasteful, ineffective intelligence program to the *Baltimore Sun* from 2006 through 2007.[46] Drake was charged with five felony counts of violating the Espionage Act for the “willful retention of national defense information” in his unauthorized possession. Three of the counts were connected to three documents found in his basement that he says he was supposed to keep because he was serving as a witness for a Pentagon Inspector General audit. The other two counts were for two documents in his email, one of which was marked “unclassified,” and the other was declassified three months after he was indicted in 2010.[47] Drake eventually pleaded guilty to a single misdemeanor charge of computer misuse for using NSA’s computer network to access information that he provided to someone not authorized to receive it.[48]

National security agencies also have a history of classifying documents after they are disclosed to the press, the public, or Congress.[49]

If the circumstances are such that you do decide to send classified information to an advocacy partner or others, tread extremely carefully. Given the serious potential legal consequences, including imprisonment, we recommend seeking advice from an experienced attorney who works for you before taking any action involving classified information. They can help you navigate this minefield and make informed choices.

It is highly unusual for advocacy organizations to have staff with security clearances that legally permit them to see classified information. They may not even have the option of destroying the disclosure, since they would be potentially destroying evidence of a crime. Some organizations want to avoid any potential liability that might result from receiving government secrets and might feel obligated to turn it in to the government, exposing the whistleblower to legal consequences if the data associated with the document can be traced back electronically or if there are other clues for the government’s leak investigators. Other organizations may be more receptive, but may not have thought through how to minimize the risks to you or to themselves. Don’t presume the advocacy partner or others you contact will be knowledgeable, sophisticated, or willing enough to shield your identity.

If you have classified information you want to disclose, an organization that is committed to protecting you would consider identifying a sympathetic member of the Senate or House intelligence committees, who is more likely to protect your identity and act on the evidence they can lawfully receive.[50] The organization could do this without coming into possession of the classified documents or information. Another alternative is for the advocacy partner to make its own unclassified summary of your disclosure to an Office of Inspector General or other authorized recipient without the classified information.

The next chapter will discuss how to shield identifying information as much as possible when communicating with others outside your agency about your concerns, whether or not classified information is involved. Though the risks vary depending on the disclosures you are contemplating and certain techniques can reduce the chances you will be identified, the path of whistleblowing—even anonymously—will always be professionally perilous.

Liberating Agency Documents with the Freedom of Information Act

The Freedom of Information Act (FOIA) is a tool that allows anyone to request records from federal agencies. Virtually all states also have some form of public records law.

For employees inside an agency, FOIA can be a tremendous tool for putting the agency on the record. The whistleblower can tutor advocacy partners about which records to seek, or even ghostwrite FOIA requests.

If you write documents as part of your job at an agency, you should try to minimize the chance these records can be withheld from public view under FOIA exemptions.[51] For example, since agencies often attempt to withhold records under the "deliberative process" exemption,[52] if you separate legal and policy analysis—which is the kind of information often covered by the deliberative process exemption—from factual information in your writing, it is harder for an agency to justify withholding a document or documents in full. For example, you could write a memo that includes a timeline of relevant facts in one section and legal analysis in another section.

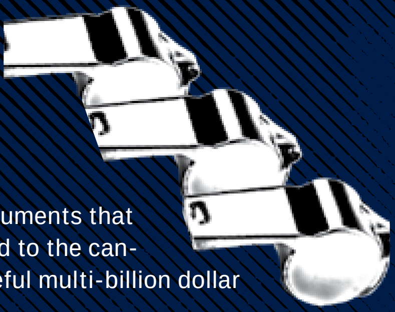
If you are receiving key records, you may consider circulating them as widely as possible without drawing unwanted attention to your action.[53] This wide circulation helps keep records available under FOIA from a multitude of sources.[54] It also makes it much harder for agencies to deny the existence of documents that have a high likelihood of turning up.

Email is another asset in the war to make government business public. Many managers write candid thoughts in emails that they would never put into formal correspondence, yet an email is just as much a public record as an old-fashioned memo is.[55] The ease with which emails can be forwarded makes email a powerful dissemination tool.

Email is another asset in the war to make government business public.

Anonymous whistleblowers can act as watchdogs for FOIA cover-ups. For example, during investigations of unsafe nuclear facilities, the Government Accountability Project worked with public employees to draft precisely targeted FOIA requests. These employees made copies of the records, and provided notice when documents were moved off-site, concealed, or destroyed.[56] Insiders have also blown the whistle to Congress on alleged abuses of the FOIA process.[57]

"ED" AND THE SUPERCONDUCTING SUPER COLLIDER



Working with the Project On Government Oversight (POGO), an anonymous whistleblower disclosed documents that ultimately generated major media attention and lead to the cancellation of the Department of Energy's (DOE) wasteful multi-billion dollar Superconducting Super Collider project in 1993.[58]

POGO only knew the whistleblower as "Ed," although that wasn't his real name. While they worked together, Ed mailed documents to POGO in plain envelopes and called the organization every other day at a certain time. Those phone calls proved to be crucial in ensuring that Ed could let POGO know what was happening, but also so that he could answer any questions the organization had about the documents he sent.

The Supercollider scandal reached a crescendo when Ed mailed POGO a draft DOE Inspector General report concluding that 40 percent of federal money spent on the project up to that point had been either wasted or misspent. Taxpayer money intended for the project had gone to pay $35,000 for a holiday party and $39,000 for coffee, among other items. Within weeks after Ed sent POGO the disclosures, the House of Representatives voted to kill the project.[59]

But no good deed goes unpunished. Then-Secretary of Energy Hazel O'Leary launched an investigation to identify the source, sending Inspector General agents with badges to POGO´s office demanding to know the identity of the whistleblower. POGO provided no information to the agents, and Ed's true identity remained anonymous, even to POGO staff.[60]

Ironically, Ed´s efforts exposing the multi-billion dollar waste ultimately led to him losing his job: the program was cancelled. He later called POGO to let them know that he was all right, had found a good new job, and was proud that he was behind the cancellation of this wasteful government contract.

It´s important to keep in mind, however, that agency officials looking to find sources of leaks could use FOIA requests as clues to identify whistleblowers through the specificity of the requested document that could only be known by key employees. This appears to have happened with then-FBI agent Terry Albury, who pleaded guilty to providing classified information to *The Intercept*. Albury disclosed to reporters a pattern of surveillance by the FBI that posed risks to civil liberties, and backed that up with information from documents showing weaknesses in the Bureau's rules against racial and religious profiling.[61] *The Intercept* filed FOIA requests for documents Albury had disclosed to it, and the FBI matched those requests up with Albury's access to many of those documents.[62]

Harnessing the Collective Voice to Shield Individuals

Union organizers know that collective action provides both power and anonymity for members of groups. While bad managers can punish individual employees for simply bringing up problems, both retaliation and smears become more difficult to carry out when a group of employees speaks with one voice.

The larger the group, the more the power imbalance is neutralized. For example, the Government Accountability Project recruited the president of the Food Inspectors Union to publicly speak in congressional testimony for a number of whistleblowers, providing cover for those concerned about harassment—a way to launder the truth on the record.[63]

Use employee surveys to document or dramatize problems within organizations without putting individual employees in the spotlight.

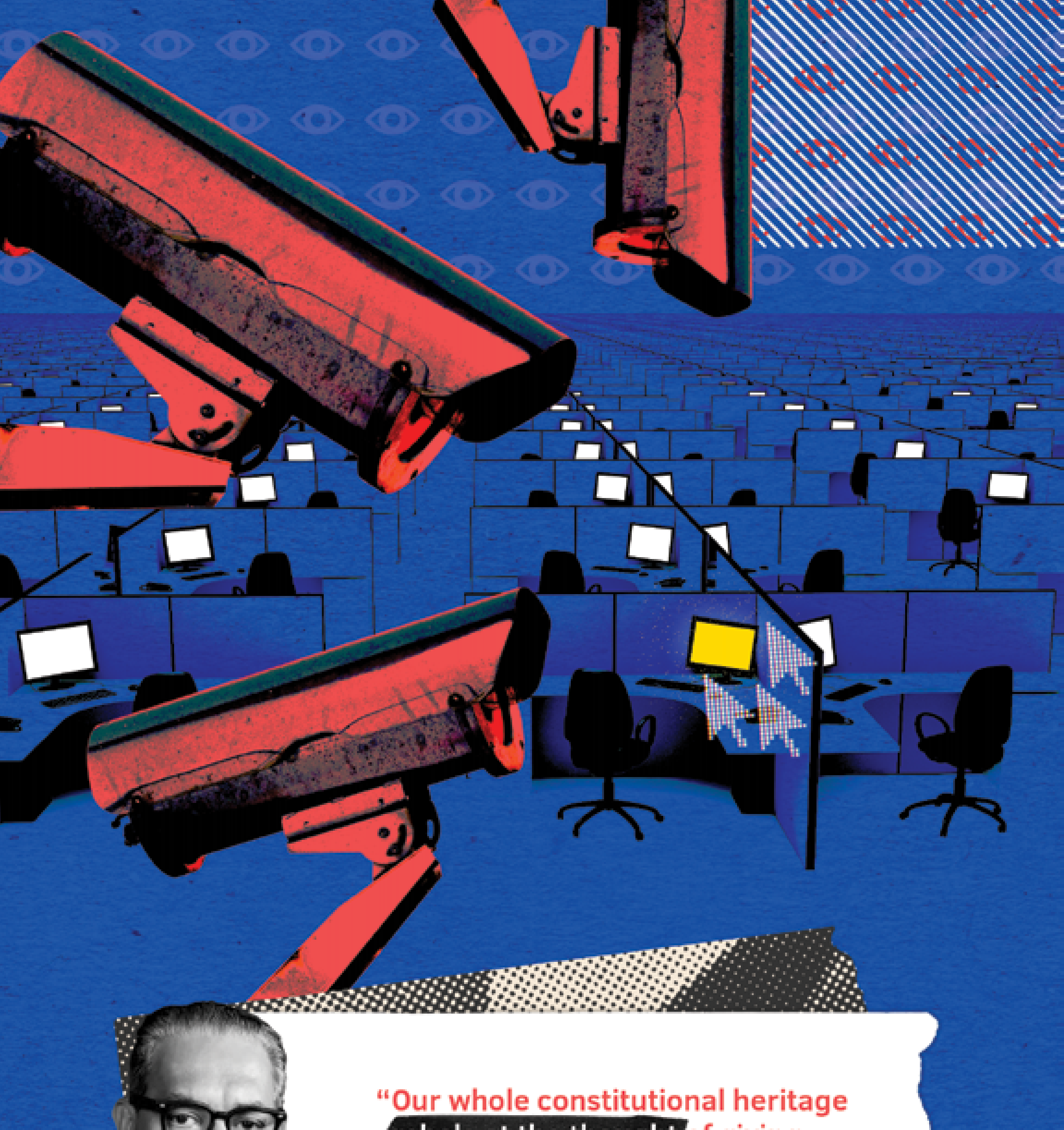
A way to put this principle into action is to use employee surveys to document or dramatize problems within organizations without putting individual employees in the spotlight. With the help of an advocacy partner, surveys can be worded with employee input to expose the most important problems facing the organization.[64]

Once the survey is finalized, an advocacy partner works with employees to distribute the questions, encourage participation, and compile the results.

The final product is a targeted audit of the organization´s leadership, fashioned by the people who best know its strengths and weaknesses.

The results are then provided to survey participants, the organization's leaders, other decision-makers, and the media. Press amplification of survey results can help keep an organization's leaders accountable, as public scrutiny can pressure leaders to address the problems identified and to make needed changes.[65]

There are other benefits to conducting employee surveys. Aside from diagnosing problems within organizations and holding leaders accountable, surveys can show individual employees that they are not alone in their concerns, reducing the sense of isolation. Best of all, if the survey is credibly designed to protect the identity of its participants,[66] this can be accomplished without threatening the job security of any employees who participate.



> “Our whole constitutional heritage rebels at the thought of giving government the power to control men’s minds.”

THURGOOD MARSHALL
SUPREME COURT JUSTICE

3

CHAPTER

Digital Security for Whistleblowers

Technology can be a valuable tool for blowing the whistle, but it can also make it easier to identify those who expose wrongdoing. While you may be able to share information with the click of a button, chances are that click will be tracked. Luckily, there are tools that can help you remain anonymous when reaching out to advocacy groups, journalists, or other potential allies online.

Digital security best practices are constantly evolving, as are detection technologies and techniques, so there are some general principles that are important to keep in mind while you decide whom and what to trust.

Think Before You Click

Always remember that digital security tools—including those reviewed later in this chapter—may mitigate risk, but they can't eliminate it. State and private actors have the ability to infiltrate many digital devices. No system is foolproof and it´s possible that previously unknown security flaws or user error, either by the whistleblower or those they are in contact with, could expose the source of the information.

The good news is that if you do your homework and are careful, some tools can help maintain the security of your conversations even if all your communications have been intercepted. Basic lessons to keep in mind are summarized below, with references for more advanced homework.

BASIC DIGITAL HYGIENE IS IMPORTANT

Almost everyone can benefit from doing a basic digital security review, even if they aren't looking into using online whistleblower tools. Taking precautions such as using multi-factor authentication to lock down online accounts and using strong unique passwords (or better yet, a password manager) can help reduce your exposure to online threats, such as criminal hackers, or government investigations seeking the source of leaked information.

SecurityPlanner.org, a tool from the University of Toronto's Citizen Lab, is an interactive guide that suggests ways you can protect yourself (and your data) online.[1] The Electronic Frontier Foundation's Surveillance Self-Defense guide is also a valuable tool that can help you to assess what digital risks you face and to find resources to offset those risks.[2] All of the tools and practices set out by these guides amount to a good baseline of security best practices, or "digital hygiene."

KNOW YOUR DIGITAL ACTIVITIES ARE BEING WATCHED AT WORK

Accessing and removing information from government systems can be as treacherous as transmitting it. Even the best encryption will not help if you already have exposed yourself as a threat. Monitoring software is widely reported to be used by employers, both in and outside the government.[3] The capabilities of such software varies, but it's safest to assume that anything you do on an employer's network or using their hardware, such as a work laptop or smartphone, can be tracked.

Be careful about what information you access at work. Many organizations consider high-tech leakers to be like hackers, and use highly advanced specialists to uncover both. Employers usually maintain logs, keep careful track of who has access to information, and monitor for unusual patterns of access.

For example, you could come under suspicion if logs show you were one of only a few people to print or email a document that later leaks. Similarly, you could draw scrutiny if you use work resources to access information related to leaking or blowing the whistle, so it’s best to do research on these issues outside the workplace not using work-issued devices, and to use some of the privacy protection tools we will discuss later in this chapter.

Be careful about what information you access at work.

In some cases it may be advisable to avoid removing data from networks directly. Some organizations automatically identify which machine accessed a file, and removing information through a flash drive, for instance, may look suspicious or even immediately trigger alarms. Consider if it’s possible to instead take pictures of the screen with a separate device under your own control. Another approach is to transcribe the information word for word on paper.

As discussed in Chapter 1, it’s important that you protect the information so investigators or journalists can later verify its authenticity. If the information is on paper, bury the original document in an archive or a file with a misleading name, or “misfile” it with documents on another topic. You may want to leave a physical copy of the information hidden somewhere secure inside the organization. Also note where the document is stored electronically and be prepared to describe the structure of your organization’s systems to whomever you are working with to blow the whistle.

If possible without revealing your identity, save an electronic copy of the file to a location where it is unlikely to be found, to safeguard against later erasure of the original. If the information isn’t time sensitive, create as long a time lag as possible between when you access the information and when you blow the whistle to reduce suspicions based on when people looked at it in the system.

KNOW YOUR DIGITAL ACTIVITIES ARE BEING WATCHED OUTSIDE OF WORK, TOO

Thanks to previous whistleblowers, including Edward Snowden, we know the government’s vast digital surveillance capabilities include collecting information about Americans’ communications.[4] Despite some transparency reforms, the classified nature of many surveillance programs makes it hard to gauge their scope.[5]

Many different entities, such as social networks, email providers, and the companies that actually provide internet access, also collect massive amounts of information about users in order to carry out their work and to fuel the online advertising market. This may include not only the content of communications, but also the "metadata"—such as what sites you visited or who you contacted and when. While the government may not have immediate access to your online activities, online-service providers may be legally compelled to turn over records in certain circumstances, such as during the course of a criminal investigation.

If you determine that whistleblowing is the right path for you, at a minimum never use your own or your employer's equipment to transmit information. Use a distant public computer at a library or internet café not likely to be associated with you. If you use a public Wi-Fi access point, avoid circumstances where you must log in or where you'll be in the view of cameras. Consider only doing research about your next steps while using some of the tools described later in this section, such as the Tor Browser or Tails.

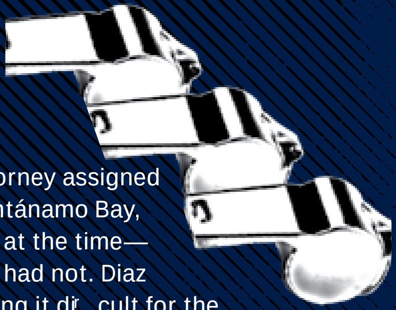
DON'T LET YOUR DOCUMENTS BETRAY YOU

Carefully consider if documents can identify you as the source before you share them. How many people within the agency have access to them? Is there identifying information built into the text such as timestamps, or tweaks to language or formatting unique to a certain version?

If you plan to share digital files, you should strip that information when possible. Tips on how to strip the info from file types such as Word documents, PDFs, and images are readily available online. Research on ways to cover your digital footprints is best done via Tails or Tor, tools that will be discussed later in this chapter, because searching for this type of information could throw suspicion on you if uncovered later during a leak investigation.

Carefully consider if documents can identify you as the source before you share them.

Scans of physical copies of documents may also include identifying information. For example, most printers leave tracking information in the form of dots not obvious to



GOING ANALOG CAN BE RISKY TOO

In 2005, Commander Matthew Diaz was a Navy attorney assigned to the U.S. naval base and detention center at Guantánamo Bay, Cuba. Over 550 men were held at Guantánamo Bay at the time—some who had committed terrorist acts, some who had not. Diaz was deeply troubled that the government was making it difficult for the detainees to have their day in court. One barrier was the secrecy surrounding the men's identities. Even though the Supreme Court had ruled six months earlier that the prisoners had a legal right to challenge their detention in court, the Pentagon insisted the detainees had no legal rights to counsel. And "keeping the names secret made it harder for volunteer lawyers to file petitions on the prisoners' behalf" to challenge their continued detention, according to *The New York Times*.[6]

Feeling a "moral obligation," as he put it, one night Diaz printed out a document filled with names and other information on the detainees, put the document inside a Valentine's Day card, and, several days later, mailed it to an attorney at the non-profit Center for Constitutional Rights based in New York City.[7] Unsure who had sent the document and what to do with it, the attorney reached out to a clerk for a federal judge presiding over a Guantanamo lawsuit. The court directed her to turn the records over to the Justice Department, and the FBI began to investigate.[8]

The *Times* reported that the FBI "had little difficulty narrowing the list of possible suspects. Diaz had printed the document from his own computer, bought the valentine at the base exchange and left his fingerprints on the list."[9] He was convicted in 2007 on charges of "passing classified information" with an "intention to harm the United States" and was sentenced to six months in prison.[10] Diaz also lost his license to practice law.[11]

A year after Diaz mailed the information to the Center for Constitutional Rights, the Associated Press obtained the names of the detained men through a Freedom of Information Act lawsuit.[12]

Diaz's story shows that an electronic trail can be left by devices we don't think about—in this case, printers. It also shows that analog methods, such as using the mail and printed documents, can also leave behind clues for law enforcement authorities. It shows that the lack of a dialogue between a whistleblower and the recipient of their information can lead to actions without the benefit of informed deliberation that put the whistleblower in legal jeopardy. It also shows that there can be legal alternatives for getting the information out.

the human eye. These should be scrubbed before the document is shared, if at all possible, through methods such as converting the document to black and white and making repeated printed copies that can distort the trackers.[13] However, be aware that most modern scanners and copiers also have internal memory that keeps a log of files they are used to produce, so use a device that is not linked to you.[14] And remember that even when taking those measures, watermarks and microdot tracers—like those that appear to have exposed Reality Winner—can be difficult to entirely remove.[15] For that reason, you may want to consider taking photos of physically printed documents or of information as it appears on your screen.

If you have managed to safely obtain a sensitive document, don't store digital copies on your personal computer or phone if possible. Also avoid cloud storage services like iCloud or Google Drive that can be linked to you. Instead, keep them isolated and encrypted on new, securely stored flash drives that have never been used on a computer that can be traced to you.

ENCRYPTION IS YOUR FRIEND

The best defense against digital snooping at this time is using technologies that incorporate strong encryption, both for communications and stored data. For communications, end-to-end encryption—encryption that applies throughout the process to help ensure that only the sender and receiver can read the contents—is currently the best tool to use. This method creates a protected digital connection between the parties of a communication who know the appropriate "key." Encrypted storage works similarly and can typically be unlocked using a passphrase key devised by the user.

However, it's important to note that the strength of the protections that encryption provides is typically based on how long it could take someone to "crack" the key by using computers to make automated guesses to unlock the data. That means that even if communications are secured with the strongest options currently available, future advances in computing may make something that would take years or decades to crack now easier to crack in the future.

Encryption can protect the content of different types of communications, including instant messages, email, and voice calls. Generally, metadata, such as when and who you contact, may still be observable because this information is necessary to deliver messages. Some encrypted-communication products mitigate that risk by retaining minimal records or logs of such data. Check the tools section of this chapter for more information.

Be sure to verify the identity of contacts before sharing sensitive information. When visiting websites, make sure they are Hypertext Transfer Protocol Secure (HTTPS). Websites that don’t have this are susceptible to cyberattacks that can be used to trick you into thinking you are sending information to a site you trust when you are actually sending it somewhere else. Private information sent via unsecured sites may also be vulnerable to snooping by other people connected to your same network.

Be sure to verify the identity of contacts before sharing sensitive information.

The Electronic Frontier Foundation offers a web browser extension to assist in preventing this problem.[16] The group’s Privacy Badger tool, along with the browser plugin NoScript, can also help make your online experience more secure by blocking digital trackers and potentially insecure parts of websites.[17]

BE CAREFUL WHOM YOU TRUST

It’s important to consider that using an encrypted communication method doesn’t stop whomever you are communicating with from voluntarily (or accidentally) sharing things further. Reality Winner was exposed when *The Intercept* shared her documents with a government agency to verify their authenticity.

Consider: would the organization or journalist you're working with be willing to resist a subpoena to protect your identity?

Before sharing records with a journalist or organization, make sure the recipient will be satisfied to authenticate the record by using other information or by proof such as supporting witnesses, not by running the document past its originating agency. Your communications may also be exposed if their (or your) devices are compromised, either through malicious hacking or a legal method, such as being forced to comply with a court order.

If you have safely accessed information, one option is to transmit that information through a tech-savvy lawyer who uses encryption best practices. In addition to the technological safeguards, you may be shielded by the attorney-client privilege if you pursue this route. However, that protection may not hold up in all situations, such as when facing Congressional inquiry.[18] A lawyer also may be able to negotiate an agreement with legally binding commitments before you turn over sensitive information to potential allies.

Research the security track records of individuals and organizations before you reach out to them. Do they use recommended encrypted communication services? Will they commit to stripping any identifying information from documents, and explain to you their process for doing so? What is their policy on responding to government demands for information, and how have they responded to past demands? Have they been the victims of hacks before? If so, what was the fallout? Have sources been compromised due to their digital security failures?

Once you’ve decided to reach out to an organization or journalist, carefully consider what you want the ground rules for your communications to be.

These questions and more will play into how much information you feel comfortable sharing with those you contact. Consider: would the organization or journalist you’re working with be willing to resist a subpoena to protect your identity? If not, do you want them to know who you are?

Once you’ve decided to reach out to an organization or journalist, carefully consider what you want the ground rules for your communications to be. Ask for concrete definitions for terms like “on background” or “off the record,” which organizations and journalists may interpret in different ways (see Chapter 5 for more on this).

USING DIGITAL TOOLS ISN'T ALWAYS THE BEST WAY

In some cases, in-person meetings may be less risky. When setting up a physical meeting, look for places without cameras and where neither you nor the person you are meeting have to sign in or are likely to be recognized. Examples include public parks, community centers, and trails.

And remember: most people now carry an incredibly sophisticated digital snooping device around with them—their smartphone. Location or other types of information tracked by devices such as cell phones (including older "feature phones"), smartwatches, or even other digitally connected devices like fitness trackers may be cross-referenced and used to help identify who a person has interacted with—*even if you turn off location tracking in your devices' settings*—so leave them at home if you set up an in-person meeting, and ask whomever you are meeting with to do the same.[19] Many smartphones also do not allow you to remove their batteries, leaving them vulnerable to potential attacks where the device may appear to be powered down, but actually is still surreptitiously collecting information. If compromised, your phone could even be turned into a video- or audio-recording bug.[20]

Cars can also be easily scanned and tracked through methods such as automated license plate readers; if you are using a vehicle associated with you to travel to a meeting, assume it can be tracked. Similarly, public transit that you pay for with a reloadable card, and apps like Uber and Lyft, collect information about your travels that could potentially be turned over to law enforcement during the course of an investigation. In some cases, going old-school and using foot- or pedal-power to get to a meeting may be the best option.

THE DIGITAL SECURITY LANDSCAPE IS CONSTANTLY CHANGING

The tools and best practices laid out in this guide are recommendations based on what is known at the time of publication. But the rapid pace of innovation in information security and the increasing sophistication of digital attacks mean things may be different by the time you are reading this. What is digitally secure now may not stay that way forever.

For example, encryption depends on the complexity of keys, but future developments in computing may make what are now considered secure keys easy to guess. Other surveillance technologies in development or on the rise may later uncover actions taken now. Just imagine future investigators using facial recognition technology against security-camera archives to look for who may have met with a particular whistleblower advocacy group or journalist.

You should research recent security news about a tool before deciding to use it for sensitive communications.

The Current Toolkit

The Electronic Frontier Foundation's Surveillance Self-Defense guide maintains walk-throughs on how to set up and use many of the tools laid out below.[21] The Freedom of the Press Foundation, a non-profit with an emphasis on protecting public-interest journalism and whistleblowers, is also a valuable resource for information about current digital best practices.[22]

Note that in almost all cases, using a digital method will create some sort of data trail. However, the tools below can help minimize and hide that trail better than using ordinary communication methods.

ENCRYPTED EMAIL: PGP

The most commonly recommended way of encrypting email is called PGP and relies on public key encryption. This can be done using a laptop or desktop computer and involves installing special software to set up encryption keys for your email account and then connecting with another person who has gone through the same process. The Electronic Frontier Foundation has a good step-by-step guide for the process. (Note that, as with other tools discussed in this section, PGP has encountered security problems in the past.)[23]

This method is effective at securing the content of email messages, but still leaves metadata, including subject lines, the sender, the recipient, and the date of a message, exposed. If you have digital records on another device, such as pictures of documents that you've taken with a camera or smartphone, you'll need to securely transfer them to the computer you're using for your PGP encrypted email before you can send them on.

Consult current online resources like the Freedom of the Press Foundation or the Electronic Frontier Foundation for best practices to minimize your digital trail.

TEXTING, VOICE CALLING, AND DOCUMENT SHARING: SIGNAL

Signal is an app that provides end-to-end encrypted messaging and voice calls. It's more user-friendly than using public key encryption to protect emails, having an interface similar to most texting or instant-messenger services.

Signal can also be used to share digital documents. Before discussing sensitive topics, you should verify the security of the connection between yourself and the other person by comparing safety numbers via the app, a process explained on Signal's website.[24] The app also includes security features, such as the ability to set expiration times for messages, which can be used to minimize the digital trail left in the wake of blowing the whistle.

Signal is available for Android and Apple smartphones, as well as for desktop computers. Signal is open source and has undergone independent security audits.[25] However, the app has also had some security problems, particularly involving the desktop client. The smartphone apps have a longer security record and have had fewer reported security issues to date.[26]

One pitfall of using Signal is that the app, even when using the desktop variant, is inherently tied to a phone number. However, there are steps you can take to reduce the risk of being identified as the user behind a specific Signal account, such as setting up a burner phone[27] and using the device only in certain locations that aren't regularly associated with you. Be sure to erase your call history, which Signal otherwise will maintain locally on your device.

Court documents related to a 2016 subpoena of the app's developer, Open Whisper Systems, appear to show that the only information retained by Signal's systems were the date an account was created and the date an account last accessed Signal's servers.[28] However, without manual or automatic deletion of messages from your devices, the conversation could still be compromised if law enforcement gains physical access to your devices.

WEB BROWSING: TOR

Tor is a network that masks your online activities by encrypting your traffic and routing it through different servers, or "nodes," around the world to make it more difficult to track. It also allows you to access special websites that end in .onion, such as those used by the SecureDrop system, another whistleblowing tool we will discuss later in this section. At the time of publication, the most accessible way to use this network is by downloading an internet browser called the Tor Browser, a version of Firefox with various security functions built into it.[29]

Although Tor is a vital tool for those seeking anonymity online, it has suffered security failures in the past,[30] and some experts believe traffic over the network may receive extra scrutiny from law enforcement or intelligence agencies.[31] Your privacy can also be compromised if you log in to services tied to your real identity during a Tor session when you are also using it to communicate with advocates or journalists.

GENERAL COMPUTER USE: TAILS

“The Amnesic Incognito Live System,” or Tails, is a free operating system designed to provide users a private computing experience.[32] It can be run on most computers from a flash drive, and it automatically incorporates encryption and other privacy-protecting tools. For example, Tails automatically routes online activities performed while the operating system is in use through the Tor network and comes preloaded with the Tor Browser to secure your browsing from prying eyes.

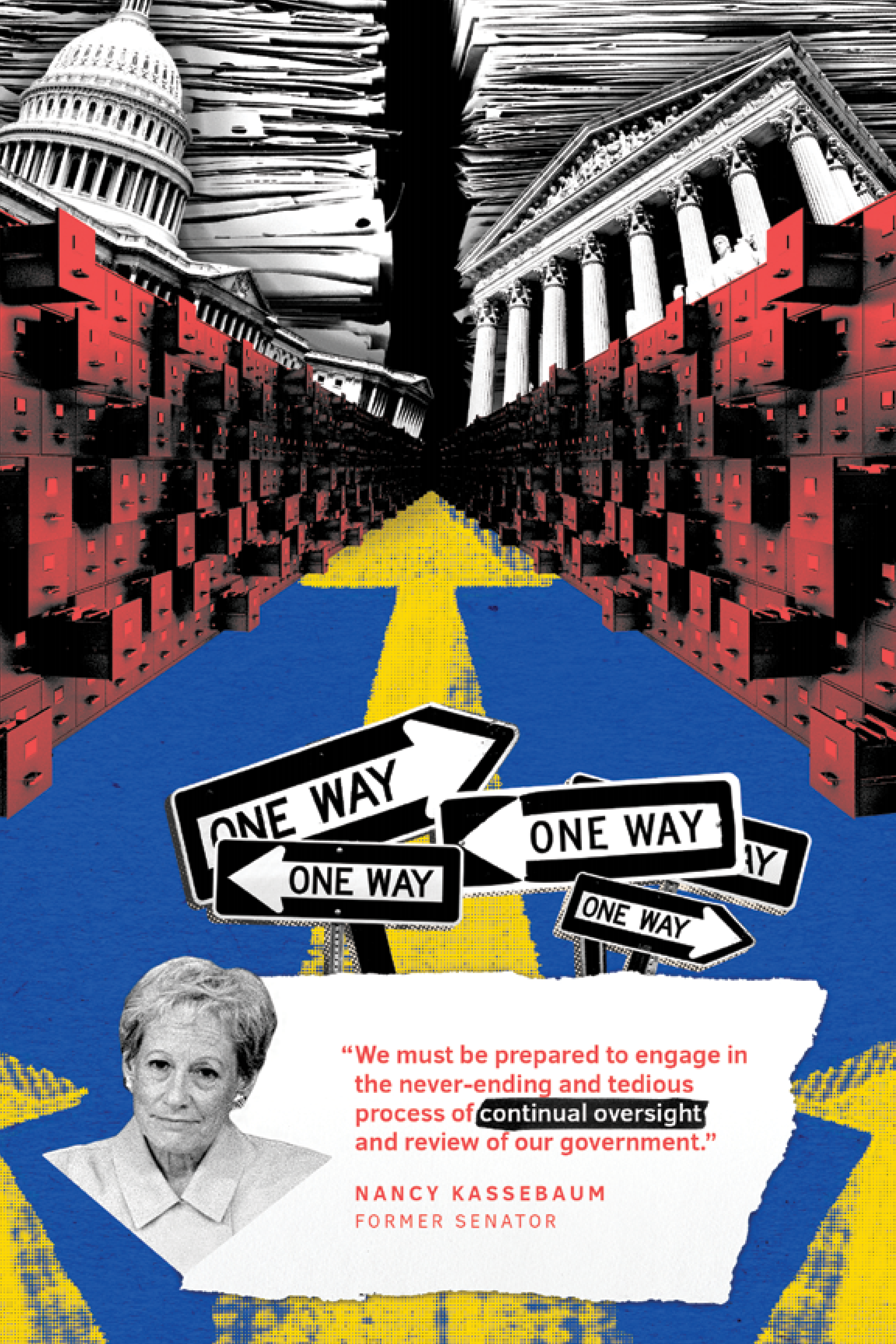
It is important to note that these added protections generally cause Tails to run slower than other modern operating systems. Tails is an open source project that is continually being improved upon, so it is important to ensure you are running the most recent version. It’s also worth reviewing the developer’s warnings about issues Tails cannot protect against before using it.[33]

SHARING DIGITAL DOCUMENTS: SECUREDROP

SecureDrop is a system designed to facilitate anonymous communication between sources and non-governmental organizations or journalists and is generally considered the most secure digital method to contact a reporter or advocacy group.[34]

Nonprofits and media outlets generally run SecureDrop on their own in-house servers and only access the encrypted communications sent through the system on computers that are running the privacy-focused operating system Tails and that are not connected to the internet, which minimizes the potential for third parties to access information shared via the system. SecureDrop also does not record many forms of potentially identifying information about submitters, such as the IP address or the type of operating system being used.

SecureDrop requires users to install and send information through the Tor Browser. The Freedom of the Press Foundation, which manages SecureDrop, recommends that whistleblowers who are sharing national security-related information go even further by using cash to purchase a new computer and connecting to the internet via public Wi-Fi that they don't normally use.[35]


ONE WAY
ONE WAY
ONE WAY
ONE WAY
ONE WAY

> “We must be prepared to engage in the never-ending and tedious process of continual oversight and review of our government.”

NANCY KASSEBAUM
FORMER SENATOR

4

OFFICIAL CHANNEL SWIMMING:

Starting and Monitoring Agency Investigations

One of the most treacherous situations for a public servant is navigating the bureaucracy of filing whistleblower disclosures. This chapter is focused on the official channels through which you can report wrongdoing. Note that filing a whistleblower disclosure is not the same thing as filing a complaint of whistleblower retaliation. The channels through which you can file a retaliation allegation are addressed in Chapter 6.

Many employees first disclose concerns to their supervisors. These employees may not intend to “blow the whistle”—they just want to let management know about a problem or have to disclose it to do their jobs properly.[1] The Whistleblower Protection Enhancement Act of 2012 protects disclosures of wrongdoing that federal employees make to supervisors or as part of their job duties (see Chapter 6 for a discussion of retaliation protections).[2] Still, if a supervisor feels threatened by your disclosure, you could end up in their crosshairs. Conversely, failing to report a problem can also lead to difficulties, particularly if the problem becomes embarrassing and the agency starts looking for a scapegoat.

If reporting the problem to a supervisor resolves the matter, great. If it does not, and you need to go to oversight bodies outside the chain of command, the water becomes murkier. When you go outside of your immediate organization, especially when your concerns become public, it heightens the chance that your management will become angry with you.[3]

Because there is the potential for retaliation when you blow the whistle, especially if you decide to file a formal disclosure outside of the chain of command, you should seek legal advice from trustworthy counsel before taking any action (although there may not be time for this, especially if you are reporting an imminent health, safety, or security matter). Legal counsel will explain what protections are available to you and how to best take advantage of them, and can also help you work with offices that may investigate your disclosure.

If you want to swim in these official channels, the following should be taken as cautionary advice.

Inspectors General

Every major federal agency has an inspector general (IG). One of an IG's main roles is to investigate whistleblower disclosures of internal fraud, waste, abuse, and other types of misconduct. See Chapter 6 to learn more about their role in investigating whistleblower retaliation claims.

An IG office generally conducts investigations and audits. You can file a disclosure with an IG through its "hotline," which can usually be contacted through phone, email, or mail.[4] The scope of an IG review depends on the nature of the issue at hand and what type of staff is assigned to your inquiry.

One of the main roles of an inspector general is to investigate whistleblower disclosures of internal fraud, waste, abuse, and other types of misconduct.

Investigators tend to go narrow but deep, and focus on individuals' misconduct, such as violations of law, regulation, or policy. Investigations that find violations of criminal laws can result in referrals for prosecutions, but whether to prosecute is a decision made by a Justice Department attorney.[5] Investigations can also lead to non-criminal, administrative penalties, such as termination.[6] Auditors look at program performance or financial management, and typically do not focus as much on individual wrongdoing.[7]

Under the Inspector General Act of 1978, IGs are supposed to be independent of the agencies they oversee. But reality doesn't always match that requirement. Some agency, commission, board, and legislative-branch IGs are appointed by the head of the organization they monitor, creating a structural conflict of interest.[8] And while IGs for most larger agencies are nominated by the president and confirmed by the Senate, giving them greater independence from their agency, those IGs still report to the head of the agency and serve at the pleasure of the president.[9] If an IG is upsetting the Administration's apple cart, they can be removed.[10]

Agency employees may view the IG as a kind of knight in shining armor—an outside, objective force charging up the hill to make all right in the agency world.[11] However, an IG office is a bureaucracy just like any other, and can have all the dysfunctions and limitations of any other workplace.[12] In fact, there have been numerous instances of whistleblower retaliation within IG offices against its own staff for raising issues.[13]

That said, there are dedicated IG staffers who fairly and aggressively work with whistleblowers.[14] An IG office also often works closely with prosecutors and Congress. Even if your plan to expose wrongdoing does not involve going to an IG, an IG may be involved at some point and you should understand the limits of these offices.

YOU SHOULD KNOW THAT INSPECTORS GENERAL:

HAVE NO CORRECTIVE ACTION POWER

An IG can identify a problem and then make findings and recommendations. The agency in question does not have to follow IG recommendations, even if the IG confirms your disclosures.[15]

DO NOT GUARANTEE CONFIDENTIALITY

The Inspector General Act of 1978 provides that an IG should keep its sources confidential unless it “determines such disclosure is unavoidable during the course of the investigation.”[16] This leaves disclosure of your identity up to the discretion of the IG (an action for which you have no recourse). It's not a theoretical possibility: IG investigators have identified whistleblowers to the whistleblower´s management, which then led to management retaliating against the whistleblowers.[17]

Even if an IG does not disclose your identity, it may give away information to management or conduct its inquiry in a way that makes your identity patently obvious.[18] If you choose to remain anonymous, you should consider negotiating signed confidentiality agreements custom-fitted to your situation. In particular, the agreement should provide that, in consultation with you or counsel, the IG will not communicate any identifiable information that can be traced back to you. Further, you should lock in a commitment to provide you with advance notice if the IG decides that release of your identity truly is unavoidable.[19]

LACK DEADLINES

An IG can investigate (or ignore) your reports of wrongdoing at its leisure. The IG controls the investigation; you do not. Thus, an IG can take years to investigate a disclosure of wrongdoing. If it completes an investigation, an IG can still sit on the report, keeping it as a "draft" until it's no longer timely.[20] An IG is under no obligation to publicly release the investigative report (though audit reports are usually made public).

AVOID CONTROVERSY

IGs sometimes seem to dwell on a $5,000 discrepancy while ignoring a $500 million issue with politically hot policy implications.[21]

CAN TAKE ACTIONS THAT ARE USED AGAINST THE WHISTLEBLOWER

It's possible that your motivation for reporting will seemingly become the subject of an IG investigation.[22] It can seem that the IG wants to discredit your whistleblowing.[23]

Congress

You may believe that problems within your agency would be solved if only Congress knew about them. In reality, a Congressional solution on its own is the exception rather than the rule.

KEEPING CONFIDENCES

There are provisions of the Inspector General Act that instruct inspectors general to protect the identities of whistleblowers.[24] But inspectors general have not always acted in a way that is consistent with the intent of the law or that creates an environment that fosters whistleblowing.

Take the case of Diem-Thi Le, a Defense Contract Audit Agency (DCAA) auditor. In 2005, she made disclosures about flawed audits to the Defense Department's inspector general.

In April 2006, inspector general investigators sent Le's supervisor a letter seeking information on 10 audits that Le had confidentially alleged were flawed. Le had been involved in six out of 10 of those audits.

According to the Office of Special Counsel—which investigated her later claim of retaliation because she faced plummeting performance reviews after her disclosure—"no other non-supervisory auditor was involved in more than two of the 10 audits."[25] A DCAA supervisor, who was found to have retaliated against Le, told the Office of Special Counsel it was 'relatively easy to connect the dots,' and figure out Le was the whistleblower based on the audits the IG was scrutinizing.[26]

Another relevant case occurred in 2014. Massive numbers of Department of Veterans Affairs (VA) insiders began blowing the whistle against the agency, and hundreds of them contacted the Project On Government Oversight (POGO) confidentially with their disclosures.[27] Many expressed a fear of retaliation if their identities were revealed, even to the VA Inspector General.

In fact, the VA Inspector General issued a broad subpoena to POGO in May 2014 seeking "all records that POGO has received from current or former employees of the Department of Veterans Affairs, veterans, and other individuals or entities relating in any way to wait-times, access to care, and/or patient scheduling issues."[28]

POGO refused, arguing that the subpoena infringed on the organization's "freedom of speech, freedom of press, and freedom of association rights as they relate to all whistleblowers and sources."[29] Senator Ron Johnson agreed and called the subpoena "highly inappropriate" and a "potential abuse of power."[30]

The VA Inspector General dropped its subpoena and never received records from POGO.[31]

While Congress sometimes conducts investigations and investigative hearings, in many cases the bulk of the investigative work was done elsewhere, such as by an inspector general, the Government Accountability Office (GAO, an arm of Congress), or an agency.[32] The official purpose of the Congressional hearing is to create a public record that can inform and build a case for legislation,[33] but it can also be used to dramatize a situation and shape what the public thinks.[34] A quintessential use of this power was the 1994 House of Representatives hearing in which tobacco company CEOs were subpoenaed to testify under oath about their knowledge of the dangers of smoking.[35]

Congress is an unquestionably political entity. It is made up of hundreds of offices led by Representatives and Senators, each with their own stakeholders and political commitments, as well as dozens of committees with different, sometimes overlapping jurisdictions over the parts of the federal government. Capitol Hill is awash with activity and intrigue where short-attention-spans and one-page summaries are common because of overwhelming workloads and a lack of time.[36]

A 2010 federal survey shows that federal employees have far less faith that Congress will protect their identity than an inspector general or the Office of Special Counsel.

If you seek to wade into the swirling eddies of Congress, you face risks such as having your identity inadvertently exposed to your agency. A 2010 federal survey shows that federal employees have far less faith that Congress will protect their identity than an inspector general or the Office of Special Counsel, an independent agency empowered to receive whistleblower disclosures from most federal civilian employees.[37]

However, Members of Congress can be great allies, and sometimes you can appeal to legislators who want to act against bureaucratic breakdowns. Legislators have access to the media and can shine a national spotlight on problems. It can be far more difficult for your organization to retaliate against you if a Member of Congress supports you.[38] As a result, a legislative partnership can be invaluable—but it is a relationship that you must craft carefully.

The first way many public employees contact a Member of Congress is by writing a letter laying out a problem or issue in their agency. That can be a mistake. What sometimes happens with letters from public employees is that the Congressional office sends a copy to the agency for a response.[39] The perpetrators of the misconduct may be the ones who prepare the agency answer, and they learn the identity of the "troublemaker" whistleblower within their midst. Before sending sensitive material to a Congressional office, you should do preliminary research and have informal discussions to pin down ground rules. Things to consider are:

- **Does the Member have a political stake in the matter?** The Member's relevant voting record could be telling, as could campaign contributions.
- **Is the Member a chairperson or ranking member of a committee or subcommittee with jurisdiction over the issue, or have they worked on the issue in another capacity?** If so, the Member may have staff who is knowledgeable and helpful.
- **Are you a constituent of the Member or close to someone who is a constituent?** Members tend to be more attentive to potential voters.
- **Does the Member have a history of working with and protecting whistleblowers?** Does the staff of that office have experience working with whistleblowers?

If you decide to approach a Member of Congress, you should:

- **Be truthful.** Members of Congress and their staff are under no obligation to work with anyone, unlike staff in oversight agencies in the executive branch specifically authorized by law to accept and review whistleblower disclosures.[40] They will quickly stop working with you if they learn you misrepresented facts.
- **Be concise in your presentation.** Their time is at a premium. You should be very clear about *precisely* what action you want taken, such as having a Member of Congress request that a watchdog agency such as GAO or an inspector general investigate your disclosure. (Members of Congress will rarely hold a hearing based on a whistleblower disclosure without official verification, so you generally should not ask for a hearing as an initial step.)
- **Realize that Congressional staff — not the Member of Congress — will be working on your case, but the Member of Congress will be the ultimate decision-maker.**

- **Do the work for staff whenever possible, such as researching documents and ghostwriting questions or communications.** In other words, “staff the staff.” This may mean preparing a file for them on your issue. The file should have a one-to-two page talking-points memo that concisely states the key conclusions supported by the most powerful facts, so that a staffer can make the Member appear as an expert during the five-minute walk from office to hearing room. It also should contain any prior media coverage, and expressions of support or concern from stakeholders whom you have recruited. Staffers will be grateful, because whether or not they agree with you their highest priority is to make sure their boss doesn’t appear ignorant or taken by surprise on something important to voters.
- **Be courteous and flexible rather than demanding, and, if the Member helps, express your thanks even if you don´t get everything you had hoped for.** You should always strive to be helpful.

If a Member of Congress or, even better, a committee chairperson, takes up your cause it is potentially a huge asset. However, be aware that no individual Member has direct authority over the executive branch. Thus, even in the face of Congressional opposition, an executive agency can still proceed to engage in the concerning activity you have blown the whistle on. That means your best ally is often one with appropriations or oversight authority over the agency in question.

Office of Special Counsel

As discussed in greater detail in Chapter 6, the Office of Special Counsel (OSC) is the main place where federal civilian whistleblowers can lodge complaints of retaliation.[41] Perhaps less known is that OSC is a place where a civilian federal employee can go to blow the whistle on waste, fraud, abuse, or other kinds of misconduct.[42] That said, OSC is not an option for some types of federal-sector employees, such as FBI and military employees.[43]

In order to report a problem to OSC, you must do the following: first, file a disclosure with OSC detailing the wrongdoing. OSC then has 45 days to review your disclosure and determine whether further investigation is necessary (note that OSC often does not meet this 45-day deadline).[44] If OSC finds there is a “substantial likelihood that the information discloses a violation of any law, rule, or regulation, or gross mismanagement, gross waste of funds, abuse of authority, or substantial and specific danger to public health and safety," OSC must immediately inform the head of the appropriate agency of the matter. That agency head is required to conduct a proper investigation into the disclosed matter. Often, the agency head tasks the agency's inspector general to conduct the investigation. The agency head has 60 days (unless OSC grants an extension) to submit a written report outlining the findings.[45]

This report must include:

- A summary of the disclosure leading to the investigation
- A description of how the investigation was conducted
- A summary of all evidence found during the investigation
- A list of any real or apparent violations
- A description of any action either taken or planned to be taken in response to any violations[46]

Upon receiving the agency report, OSC is required to review it and determine if it contains the required information and whether the findings are reasonable. OSC has to transmit a copy of the agency report to you unless it referred the matter to the Justice Department as a potential criminal case. You have 15 days after receiving a copy of the agency report to submit comments on it to OSC. The Special Counsel then grades the report. If dissatisfied, the OSC either can direct the agency to provide more information, or simply flunk the effort.[47]

OSC transmits the agency report, your comments, and its own evaluation to the president, Congressional leadership, and the Congressional committee(s) with jurisdiction over the agency. OSC also makes these materials available to the public online.[48] If OSC does not receive the agency report within the allotted time including extensions, OSC is required to submit all available information to the president and the proper Congressional committee(s) along with a statement noting the agency failure to file its investigative report.[49]

The disclosure process has several strengths and weaknesses.

Strengths:

THE AGENCY IS FORCED TO DEAL WITH YOUR ALLEGATIONS.

An agency may try to ignore threatening whistleblowing disclosures as long as possible, simply not acknowledging their existence and hoping the issue will blow over. When OSC orders an investigation, the agency no longer has that choice.

THERE IS OVERSIGHT OF AGENCY INVESTIGATIONS.

Outside of the OSC process, when an agency acknowledges the existence of your concerns, it may respond with a quick report that rewrites or brushes aside hard issues and ignores significant evidence. This allows the agency to declare the issue was investigated and to let itself off the hook. Moreover, your contributions and evidence are often not recognized in the official record.

The OSC disclosure process, which gives you a formal opportunity to provide input on the investigation they spark, makes it harder for an agency to brush your disclosures aside. The law requires the agency to investigate your allegations and detail all material evidence it uncovered during its investigation in its report. The report also must include findings that take a stand on whether misconduct occurred, and what if anything the agency will do about it.[50] Your comments are officially made part of the record in full, and OSC makes an independent determination as to whether the resolution was responsible.[51]

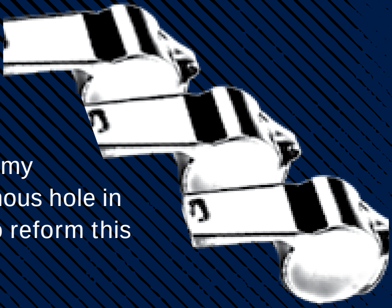
THE PROCESS CAN VINDICATE AND PROTECT THE EMPLOYEE.

If OSC makes the finding of “substantial likelihood,” it is certifying that your allegations are credible.[52]

An OSC “substantial likelihood” finding provides a hook for the media to tell a story they may have otherwise ignored. Your story becomes less of an editorial risk to publish or broadcast once it has been validated to a certain extent by a government agency. The hook for several national nightly news stories on food safety, environmental threats, and national security breakdowns has been an OSC “substantial likelihood” finding.[53]

Also, it can be easier to successfully claim retaliation if agency management takes adverse employment actions against you in the wake

ONE PERSON CAN MAKE A DIFFERENCE



Dr. Donald Sweeney, a senior economist with the Army Corps of Engineers, single-handedly blew an enormous hole in the Corps’ credibility and unleashed a movement to reform this powerful but little-publicized agency.[54]

In a disclosure he filed in 2000 with the Office of Special Counsel, Sweeney revealed a secret plan by Corps officers to manipulate cost-benefit studies in order to justify building a billion-dollar expanded lock system on the Upper Mississippi River.[55] This plan—which would have had far-reaching environmental impacts on one of the nation’s most fragile ecosystems—indicated that the Corps’ decisions were based on a desire to appease the barge industry.[56]

Sweeney’s detailed disclosures, which included internal emails and memos, generated press coverage, Congressional inquiries, and raised questions about oversight and management of the Corps.[57]

Sweeney revealed memos from Corps officers that stated that the Corps would have “to get creative” in order to get funds for the Upper Mississippi project.[58] Another memo advised that if economic data failed to “capture the need for navigation improvements, then we have to find some other way to do it.”[59]

The implications of the internal emails and memos Sweeney disclosed went well beyond the Upper Mississippi. The documents revealed an entire Corps planning process driven by a desire to please industry and its friends in Congress.[60]

Public Employees for Environmental Responsibility filed Dr. Sweeney’s affidavit with the Office of Special Counsel, which found that his allegations of violations of law and gross waste of public funds had “a substantial likelihood” of validity and ordered then-Secretary of Defense William Cohen to immediately investigate the matter and to report the findings.[61] Investigators confirmed Dr. Sweeney’s allegations, finding the Corps had cultivated “an atmosphere where objectivity in its analyses was placed in jeopardy.”[62]

of the disclosure referred by OSC. The "substantial likelihood" finding exceeds the "reasonable belief" standard that is generally the threshold to qualify for anti-retaliation protection.[63]

THERE IS A CONFIDENTIALITY OPTION.

OSC is not allowed to disclose your identity unless you consent or it feels disclosure of identity is necessary due to an imminent danger to the public or an imminent violation of criminal law.[64] If the process protects your identity, it can be a very effective way to shield you from retaliation (but not always).

Limitations:

OSC DOES NOT MEET ITS OWN DEADLINES.

The small OSC disclosure unit is hopelessly backlogged. That means that scores of agency-employee disclosures languish for months and even years without action.[65] Even when OSC forwards disclosures to the agency, OSC can allow the agency extension after extension so that the 60-day agency response period routinely results in delays of a year or longer. This can make an investigation less likely to succeed: during a delay, agencies can destroy evidence, people's memories can grow fuzzy, and officials responsible for wrongdoing or witnesses to their wrongdoing may leave the government. (OSC and inspectors general cannot compel individuals who are not currently government employees to cooperate.[66])

THE PROCESS HAS NO TEETH.

While the OSC disclosure process may be an excellent transparency tool to highlight wrongdoing, OSC has no corrective power to force the agency to desist from waste, fraud, or abuse.

CONFIDENTIALITY CAN BE ILLUSORY.

An agency may figure out your identity even if you requested confidentiality from OSC because the agency will associate you with the issues OSC is requiring that the agency investigate. See Chapter 6 for more information on retaliation protections, how circumstantial evidence

WHO WATCHES THE WATCHERS?

In some cases, federal offices dedicated to upholding government integrity have their own problems, including corrupt or unethical leaders. Whistleblowers are often key to exposing wrongdoing inside these watchdog offices.

Under Scott Bloch’s tenure as special counsel from late 2003 through 2008, employees within the Office of Special Counsel (OSC) blew the whistle on his actions, disclosing mass dismissals of whistleblower cases without adequate investigation. Another act that insiders disclosed was that Bloch had created a new field office in Detroit to which he wanted to “ship out” homosexual employees from D.C. Additionally, Bloch “hurriedly” changed the agency’s long-standing interpretation of civil service law to exclude protections for LGBT federal employees.[67] In 2005, represented by the law firm Bernabei and Katz, the Project On Government Oversight, Public Employees for Environmental Responsibility, and the Government Accountability Project joined with OSC whistleblowers to file a complaint against Bloch for committing prohibited personnel practices—the very prohibitions Bloch was himself supposed to prevent and investigate.[68] In 2008, the FBI raided the Office of Special Counsel to seize records and find out if Bloch was destroying records relevant to a Congressional investigation.[69] In 2010, Bloch pleaded guilty to withholding information from Congress.[70]

Whistleblowers were also instrumental in putting a spotlight on unethical acts by the top watchdog at the Department of Homeland Security (DHS). They disclosed to the Senate that Charles Edwards, the acting inspector general at DHS from 2011 to 2013, inadequately protected his office´s independence, abused his office´s resources, sought legal advice from DHS rather than his office´s counsel, and altered oversight reports in ways that “did not comport with standard [Office of Inspector General] processes,” according to a 2014 Senate investigation.[71] One audit report on acquisition was not published. A “senior official believed it appeared that Mr. Edwards delayed the report out of a concern for his relationship with the Undersecretary for Management, who had recently hired Mr. Edwards’ wife,” the Senate report stated.[72] A separate government review found that Edwards “failed to disclose his wife’s employment…which appeared to impair the independence of a DHS-OIG audit that cost the government $659,943.32 and resulted in the rescission of the audit report.” Edwards also had staff work on taxpayer-funded time on his doctoral dissertation.[73] He stepped down from his role at the end of 2013 after his office produced records requested by Senate investigators.[74]

can be used to establish management's awareness that someone is a whistleblower, and how perceived whistleblowers are protected too.

The False Claims Act and Other Bounty Programs

If you have non-public information that a company is defrauding taxpayers in Medicare or a government contract or grant, you may be able to sue under the False Claims Act to recover taxpayer dollars.[75] While the law has been used mostly by insiders working in the private sector whose companies do business with the federal government—such as defense contractors and drug manufacturers—some government employees have also been able to use it after reporting the fraud internally.[76]

If False Claims Act lawsuits are successful, whistleblowers are entitled to a percentage of the funds recovered for the U.S. Treasury, from a ten percent minimum to a 30 percent maximum of the monetary penalties enforced. There are certain requirements that must be met in these lawsuits, also known as *qui tam* actions: the individual filing the suit must be an original source basing the disclosure on non-public information. The lawsuit, the information within it, and the whistleblower´s role in filing the suit must also be kept secret until the Justice Department has had a chance to determine if it wants to join the suit.[77] Since that can take years, ironically whistleblowers can be gagging themselves through this option.

There are attorneys who specialize in *qui tam* lawsuits, and due to the technical nature of this area of litigation, we highly recommend that you work with an experienced attorney in this field if you´re considering a False Claims Act lawsuit.[78]

The False Claims Act contains anti-retaliation provisions as well, which are discussed briefly in Chapter 6.

There are also bounty programs in some federal agencies. The 2010 Dodd-Frank law, which was modeled partly on the False Claims Act,[79] created bounty programs for those disclosing violations of law that lead to enforcement penalties greater than one million dollars at two agencies responsible for protecting financial markets ˆ the Securities and Exchange Commission (SEC) and the Commodities Future Trading Commission (CFTC).[80]

The main difference from *qui tam* actions is that the former are “private attorney general” actions where the whistleblower, alone or with the government, must fight and win the battle against fraud. While the Dodd Frank bounty rewards also range from 10 to 30 percent of penalties greater than $1 million, whistleblowers do not have to participate in the trial. They are rewarded merely for giving evidence to the government. Most significant for this guide are the carefully constructed provisions in Dodd-Frank and its implementing regulations for anonymous and confidential disclosures. Whistleblowers can make anonymous disclosures, but they have to do so through counsel if they want to be eligible for an award.[81] If they receive an award, their identity must then be disclosed to the enforcement agency, but the SEC and the CFTC are prohibited by law from publicly revealing the whistleblowers' identities, even at that point.[82]

As with False Claims Act lawsuits, government employees can make disclosures through these bounty programs. Also similar to the False Claims Act, the disclosures must involve company misconduct, not government misconduct.[83]

PRESS RELEASE
For immediate release
FIGHT
"We must not confuse dissent with disloyalty."
EDWARD R. MURROW
BROADCAST JOURNALIST

5

The Medium is the Message[1]

The media is an effective tool to influence decision-makers. It can bring transparency to government agencies and shape public opinion. Government leaders are both senders and recipients of messages via the media. For these reasons, the media alternately is respected, exploited, and feared by politicians and heads of agencies.

The media can play the role of a leveler. It can bring disputes about misconduct out of the secret world of bureaucrats and into the glare of public attention. Media coverage can show the world that someone the agency is portraying as a workplace “troublemaker” is actually a public hero, or can force the resignation of a corrupt agency head who had previously been untouchable. But media exposure can also cause an agency to change its stance on negotiations with an employee from constructive and open-minded to antagonistic and closed as it finds itself on the defensive in an embarrassing public fight.

While the media can be powerful, the effects of its coverage can be evanescent. The attention span of the public and our leaders can be distressingly short, especially in this era of the 24-hour news cycle where people consume information immediately through fast-paced social media and online news outlets, but rarely have time to digest everything they consume.

Try not to let the excitement or ego boost from media coverage undercut the point of your publicity — exposing and fixing problems. The news media frequently focuses its stories on individuals, and any stories about you may not stress the issues you are raising. And media attention is often fleeting. The cliché is true: today’s headlines are tomorrow’s fish wrap. New distractions compete daily for media attention, and the news media is a competitive business, driven by financial as well as informational dynamics, so you want to make the most of its attention while you have it.

If It Bleeds, It Leads

The saying “if it bleeds, it leads” reflects the value that the news industry places on gore. By contrast, stories about government bureaucracies or complex scientific or technical issues rarely elicit the same widespread media interest or keep viewers’ attention. And telling those stories in a compelling and succinct way can be challenging, particularly on television. As a consequence, coverage of complex or “wonky” issues is usually confined to less-sensational print or online media. Only occasionally do internal agency stories cross over from specialized publications or websites into mainstream news coverage.

Media attention is often fleeting. The cliché is true: today’s headlines are tomorrow’s fish wrap.

This means that the interest in any story about an internal agency scandal may be limited to a handful of journalists. In order to identify that limited pool and work with them effectively to educate their readers, consider the following tips:

- **Decide beforehand what your role will be.** Professional journalists need to feel confident that their sources are solid and that the documents they provide are real. Do not contact a reporter until you have made up your mind about whether you want to be quoted in the story or to be an unnamed source. It is vital that you know which ground rules you want to govern the interaction. Be prepared to explain why you want to be anonymous if you do, and consider whether there may be other people you can recommend the reporter talk to in order to substantiate your concerns, on or off the record.

- **Think about whether to let even the reporter know your identity.** Reporters usually know who their “anonymous” sources are. This information can help them assess a source’s credibility—an extremely important consideration if the whistleblower’s information could lead to a high-profile, hard-hitting story that an agency may aggressively push back on.

- **Know the outlet.** Try to figure out whether national or local outlets are the best fit for what you are trying to accomplish. The newspaper or other outlet may have business ties (such as substantial advertising buys or sponsored events) to the entity whose misconduct you are trying to expose. Research what kind of coverage, if any, your issue has garnered in the past. Look at the outlet’s relevant editorials on the issue. Look at whether that outlet has done investigative work in the past, and whether it carries critical stories that challenge agency statements.

- **Know the reporter.** Read several articles by the reporter written over time about this or a related issue and look at their social media profiles to see what interests or biases they may have. Compare the reporter’s work on a story with that of the competition. See whether your concerns are similar to issues that the reporter has highlighted, and whether that reporter does follow-up work. Consider the writer’s tone—it can be very telling. While the facts may all appear in the story, the tone can lead the reader toward one side of the story or the other.

- **Get familiar with the reporter’s ground rules.** Reporters generally accept information on three levels: off the record, on background, and on the record. Unless you negotiate a different condition in advance, a reporter will assume everything you tell them is on the record and they can use it however they want. It is too late if you wait until after an interview or other interaction with the reporter to set the ground rules. If you try to place restrictions after sharing the information, the reporter may cooperate as a favor but they are not bound to do so.

Make sure you both share an understanding of what each of the levels means and entails before you share sensitive information. Asserting something is on background or off the record in an email, without the journalist agreeing to those terms, may not be sufficient. We provide the general definitions for “off the record” and “background” below. But it’s always a good idea to verify those definitions with the specific reporter you might work with before you expose your identity or your evidence, since journalists don’t consistently agree on the definitions.[2]

> *Unless you negotiate a different condition in advance, a reporter will assume everything you tell them is on the record and they can use it however they want.*

The definitions below largely reflect how they are interpreted by the Associated Press.[3]

“Off the record” means that your name cannot be used, and you cannot be quoted. It also means that journalists cannot publish the information you provide (unless a different source independently provides the information to them). This information can help a journalist climb the learning curve, but it cannot be exposed or referenced in reporting. You should go off the record if the information you tell the reporter — regardless of whether your name or general information about your position was mentioned—would likely identify you as the source if the information were it to be published or relayed to your agency. You should let the reporter know up front whether and how, if they use the information you give them to ask questions to other sources, they could inadvertently tip off an agency that a whistleblower is talking to the reporter.

“On background” (“not for attribution” is similar) means that your name cannot be used, but that the information you provide can be published under terms that you negotiate with the reporter. This should be for information that is an essential part of the story and could be provided by people other than you (so you won´t be identified as the source) but you think should not be attributed to you by name. This is typically seen in news stories attributing information to “senior administration officials.” On background can mean many things and it is especially important to have a conversation with the reporter about what you’re comfortable with. Are you okay if the information is sourced vaguely to you but not by name (such as “an employee in the agency who does not want to be named out of fear of retaliation”)? Would you rather a reporter simply use the information to get official confirmation or confirmation from other insider sources? Most serious news organizations will not base reporting on a sole anonymous source.

“On the record” means whatever you say can be quoted and attributed to you by name.

- **Pin down confidentiality before sharing any information.** Depending on the nature of the information you provide, the issue in question, and a reporter’s ability to get information out of an agency through official channels, you and the reporter may have multiple conversations about how your information can be used.

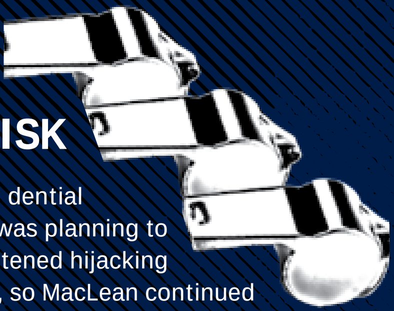
If you choose to remain anonymous, you may want to start out with an “off the record” interview and later ease into an “on background” interview as you grow more comfortable with a journalist. But wherever you start, you should be cautious when interacting with the media and be clear in each conversation on what basis you’re providing information. It can be easy to assume all conversations are covered by a previous agreement, especially if you talk to the reporter repeatedly.

When whistleblowers are casual about the ground rules, too often their identity gets involuntarily “outed.” Reporters have quoted whistleblowers who thought they were speaking off the record or on background but who had failed to pin it down. Such mishaps occur, and once that media bell is rung, it cannot be un-rung.

Even if you are clear about the ground rules, you are always taking a risk that your identity will be compromised when you go directly to the press. In rare cases, an overzealous or sloppy journalist mistakenly has named an off-the-record source. More frequently, the identity of the whistleblower becomes known through a revealing description of the unnamed source.

Talking to a reporter about how to protect your confidentiality can also help them avoid inadvertent mistakes when trying to verify documents.

- **Have the story prepared.** Start by visualizing the headline and lead paragraph of the news story you would like the reporter to write,



A REPORTING MISTAKE CAN PUT YOUR CAREER AT RISK

In 2003, federal air marshal Robert MacLean's confidential disclosure to MSNBC showed that the government was planning to reduce security on airlines during a period of heightened hijacking threats.[4] These policies put the flying public at risk, so MacLean continued to make disclosures about those policies. When he went on *NBC Nightly News* in 2004, the television program shielded his face but failed to camouflage his voice. The agency discovered his identity and also asked if he made the 2003 disclosure. He admitted to it and his agency fired him in 2006, charging him with releasing "Sensitive Security Information."[5]

After a years-long legal battle, throughout which he was represented by the Government Accountability Project and supported by the Project On Government Oversight, his case ended up at the Supreme Court, where he prevailed in 2015. The Court ruled that the Whistleblower Protection Act does not exclude disclosures made to the press or public unless the information is classified or otherwise prohibited by statute from public release. The information MacLean disclosed to the press was neither classified nor protected from disclosure by statute.[6] While he was reinstated in his agency, as of this book's publication, his employment struggles with management continue. His agency has ordered him to take psychiatric examinations, delayed processing his security clearance for over a year, placed him under criminal investigations, and proposed to terminate him—which all began because *NBC* concealed his name and his face, but not his voice.[7]

The lesson here is that in order to truly conceal your identity you must think through the myriad ways an agency can figure out who you are and make sure the organization you are working with is as detail-oriented in protecting your identity as they need to be. A simple mistake can lead to huge consequences.

By establishing ground rules with a journalist, you can help reduce the risk of them unintentionally compromising your identity. For example, a court document suggests that a reporter unintentionally blew the cover of National Security Agency whistleblower Reality Winner in 2017, at least in part because the reporter shared a classified original document he received from Winner with the government in an attempt to verify it. Though Winner had anonymously mailed the classified NSA report on Russian attacks to *The Intercept*, an online news outlet, the government was able to identify that she was one of six individuals who had printed the report.[8]

The reporter should have known the risks of sharing the document, but sources are often in the best position to communicate sensitivities the media might miss or overlook. Other government or contractor employees with security clearances who could verify the accuracy of information may feel obligated to report a potential breach of national security. As *The Washington Post's* media critic Erik Wemple wrote, "It's apparent that the document came straight out of the blue, with little or no instructions as to sensitivity and handling."[9] Such instructions, perhaps, could have helped Winner avoid jail time.

including why the information you are providing matters to a broader audience. Start with your bottom line. Write a short, to-the-point summary and back it up with definitive documentation. Respect that the reporter has limited time, so make the research as easy as possible.

The key to publicizing problems within an agency is to make the story interesting and clear, so present reporters with a compelling description of the problems and their ramifications for the media audience. That means emphasizing consequences in language that will create an image for readers. Adjectives like “horrible” and “tragic” are not news. But it is news if a town could become rubble or a crater. Remember to keep the emphasis on the story, not on yourself.

- **Set a deadline.** Try not to leave the timing completely up to the reporter; if you do, you may find yourself frustrated. Some television networks will keep a completed story “in the can” until “sweeps” week, when they can use it to get the best ratings. By then, however, the abuse of power may be a *fait accompli.* If the information is time-sensitive (for instance, you are trying to prevent a likely accident or tragedy, or affect an upcoming agency action or decision), you should make that clear to the reporter in your first interaction. Try to get a commitment, or find someone else whose schedule will make the story relevant as more than a history lesson. If there is a pending action, that usually helps a reporter prioritize your story and make the case to their editor about the news value of your disclosures. Most reporters have no shortage of items competing for their attention.

You may have access to trustworthy journalists and choose to contact them on your own, but it is usually much easier and more effective to partner with an advocate who can make those contacts on your behalf. Advocacy groups have experience working with the press and often keep tabs on journalists who cover specific topics or “beats.” These groups can also help package your information and put your story into a larger policy context than you may be able to do on your own.

Not every internal agency dispute or problem will merit media coverage.

Keep in mind that following these steps does not guarantee a news story.

Not every internal agency dispute or problem will merit media coverage. Moreover, even if the issue is covered, you may not like the result.

Reporters Are Not Your Friends

The best reporters add value and context to information that whistleblowers provide to them. They can also bring information to the attention of senior leaders more effectively than more-junior public servants. In some instances, by refusing to take no for an answer (or a non-answer for an answer), a reporter can take a story far deeper and have much greater impact than you ever thought possible. They can also be invaluable resources for sharing or trading evidence, and referring other whistleblowers to you or your advocacy-organization partners.

That said, the reporter is not your friend, advocate, or supporter.[10] It is not the reporter's job to find you a lawyer, to get your job back, or even to right a wrong. The reporter is just supposed to report the news accurately and fairly. Part of that process is likely to include challenging or fact-checking your allegations.

Reporters working for news organizations are not free agents. They work in a business with a chain of command and idiosyncrasies, perhaps just like your agency.

Consequently:

- **An editor may veto or cut a story.** A reporter who tells you they are committed to writing a story cannot actually guarantee when it will be printed, that it will be printed in its entirety, or that it will be printed at all. Often, a reporter's editor will cut parts of a story, even if the reporter thinks it contains key facts or analysis. Further, reporters usually do not write the headlines; a hard-hitting story may be introduced with a painfully boring—or worse, inaccurate—headline.

- **The agency may get equal time.** In almost all cases, reporters and their editor will want to include the agency reaction or explanation as part of any story. The result may come out appearing as a "he said/she said" standoff, leaving it to the reader to guess who is right. (This is where your familiarity with the tone of the outlet is particularly valuable.)

- **The agency may be able to preempt your story.** As the government, the agency has the advantage of being able to, on occasion, make news through an announcement or other action. Astute agencies have been known to release an announcement or other breaking news out the front door of their public affairs office to distract from the bad news coming out the back door from employees.

Yesterday’s News

Rarely is media coverage an end unto itself. Rather, it is just one component of a larger effort.

Sometimes the moment of greatest leverage with an agency is just before a news story runs because the agency may be willing to take steps it would otherwise not take in order to avoid or mitigate the media exposure. Conversely, the day after the story runs, the agency may be set in a defensive posture, unwilling to take any steps that imply an admission of guilt.

If your goal is to correct a problem, you should have a strategy for how to accomplish that and precisely what role media coverage will play. In other words, it is important to think of the process in terms of a campaign. This is another reason why it can be to your advantage to partner with advocacy groups that can help ensure your story reaches the audiences necessary to effect change. Very few problems within agencies evaporate simply because they have been the subject of one article in a newspaper. Most agencies can shrug off one story, or even one week’s worth of stories. It may take sustained media exposure to effect change.

Very few problems within agencies evaporate simply because they have been the subject of one article in a newspaper.

If sustained coverage is necessary, you must plan for an entire campaign and not just the first step or a single story. It can be very difficult to garner sustained media attention. Reporters may think your concerns merit only one or a handful of stories based on the information you give them. In this scenario, you need a strategy to keep up the pressure. That may include working with advocacy groups or a Member of Congress to spark an official investigation or audit of an agency, or to question the agency during a hearing. These actions may help you make your case that an agency needs to rectify the issue, especially since agencies can often waive off news reports alone as biased and slanted. But it's harder for an agency to ignore, for instance, an inspector general's report that confirms news reporting.

The key to earning public solidarity is sustained exposure of steadily accumulating evidence. That means pacing your releases of evidence. If you use everything at once, you're likely to get one story that's a blip. Your goal is to expose the story that won't go away, generating progressively less credible denials and cover-ups.

In order to generate a series of stories in any scenario, you must assemble a lot of raw material and then refine it down to individual stories. Once you assemble an arsenal of "ammunition," you should release pieces of it separately so that each salvo reinforces the effects of the one before it. If you can pace the intervals between "hits," you can give the agency ample opportunity to do something counterproductive, such as putting forth a demonstrably untrue fact in its defense, instituting a "gag" order forbidding employee contact with the media, or otherwise overreacting in a way that may be newsworthy as well. Similarly, you can intersperse releases of new evidence with other developments such as letters or expressions of support from political leaders, which can be their own complementary news hooks.

It may be that a single journalist will be interested in every piece of ammunition, but if that single journalist loses steam, approaching other outlets can increase pressure on an agency. That said, recognize that journalism is a very competitive field and a reporter may feel burned if they feel like the source is playing them against their competitors. Some journalists also won't be interested in covering what they view as the "scraps" that their competitors didn't pursue, or will simply feel like the story has already been sufficiently covered and doesn't merit their time.

If your goal is to correct a problem, you should have a strategy for how to accomplish that and precisely what role media coverage will play.

If you conduct your campaign successfully, the deepest wounds to the agency will be self-inflicted. If the wrongdoing involves the leadership of an agency, including leadership's failure to meaningfully address problems, after a few weeks or months of unrelenting bad news, media accounts may start to refer to the agency head as "embattled" or "beleaguered." At that point, support for the agency may erode as political patrons shrink away from the prospect of guilt by association.

Sustained media attention also tends to spawn official investigations (see Chapter 4) that put even more pressure on agency leadership. Each investigation not only becomes a new, separate story, but each may provide a new forum to air allegations and be a magnet for new witnesses who are starting to hope that something can be done. Each new story will recount the previous developments, like an arrest rap sheet, so that the allegations continue to build toward a climax.

Media attention can also backfire. If you are still working inside an agency and are thinking about working with the press, extreme caution is in order. The agency leadership will correctly see its professional survival at stake and critical coverage can get deeply under their skin. Breaking ranks to go public often is viewed as an act of unforgivable betrayal. Even if you were initially able to raise your concerns anonymously, you may eventually be revealed by the new spotlight you've created.